# Cisco uBR7200 Series Universal Broadband Router Software Configuration Guide

Cisco IOS® Software 12.3 BC, 12.2 BC, 12.2CX, 12.1 EC
November 2006

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-2239-05

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

*Cisco uBR7200 Series Universal Broadband Router Software Configuration Guide*
Copyright © 2004–2006 Cisco Systems, Inc. All rights reserved.

# CONTENTS


Preface xi

- Document Revision History xi
- Document Objectives xi
- Audience xii
- Document Organization xii
- Conventions xiii
- Terms and Acronyms xiv
- Related Documentation xvii
  - Cisco uBR7200 Series Documentation xvii
  - Cisco Cable Modem Termination System Reference Documentation xviii
  - Related Cisco IOS Release Documentation xviii
  - Additional Documentation Resources xviii
- Obtaining Technical Assistance xix
  - Cisco.com xix
  - Technical Assistance Center xx

CHAPTER 1 Overview of Cisco uBR7200 Series Software 1-1

- Cisco IOS Releases and Images for the Cisco uBR7200 Series 1-2
  - Determining Your Cisco IOS Software Release 1-2
  - Upgrading to a New Software Release 1-2
  - 12.3 BC Release Train Images and Requirements 1-3
  - 12.2 BC Release Train Images and Requirements 1-4
  - 12.2 CX Images and Requirements 1-5
  - 12.1 EC Images and Requirements 1-7
- Cisco uBR7200 Series Chassis Overview 1-8
  - Cisco uBR7200 Series Universal Broadband Routers 1-9
  - Supported Hardware on the Cisco uBR7200 Series 1-11
  - System Interoperability 1-14
- Cisco uBR7200 Series Router Configuration Overview 1-15
  - Port Adapter and Line Card Slot and Logical Interface Numbering 1-15
  - MAC-Layer Addressing 1-17
  - Cable Interface Line Cards 1-17
  - Cable Interface Line Card Slots 1-19
  - Interfaces and Physical Ports 1-20

Port Adapter Slots 1-20
Supported Software Features for the Cisco uBR7200 Series 1-22
Cisco uBR7200 Series Router Features and Cisco IOS Releases 1-22
Cisco uBR7200 Series Router Configuration Tools 1-31
Bandwidth Management Features 1-33
Cisco IOS Command-Line Enhancements 1-33
Cisco Quality of Service Features 1-45
DHCP Servers and Feature Support 1-47
DOCSIS 1.0 Feature Support 1-49
DOCSIS 1.0+ Feature Support 1-56
DOCSIS 1.1 Feature Support 1-57
DOCSIS 2.0 Feature Support 1-67
High Availability Features 1-68
Intercept Features 1-72
IP Broadcast and Multicast Features 1-79
IP Routing Features 1-80
Management Features 1-86
Multicast Features 1-98
PacketCable and Voice Support Features 1-101
Security Features 1-102
SNMP Features and Enhancements 1-109
Spectrum Management and Advanced Spectrum Management Features 1-119
Testing, Troubleshooting and Diagnostic Features 1-123
Virtual Interfaces 1-125
VLAN Features 1-126
VPN and Layer 2 Tunneling Features 1-126
WAN Optimization and Services Features 1-131
DOCSIS and CMTS Interoperability 1-137
DOCSIS NTSC Cable Plants 1-137
EuroDOCSIS Cable Plants 1-138
DOCSIS-Compliant Downstream Signals 1-139
DOCSIS-Compliant Upstream Signals 1-140
Traffic Engineering 1-142

CHAPTER 2 Configuring the Cable Modem Termination System for the First Time 2-1
Configuration Fundamentals for the Cisco uBR7200 Series 2-2
Preconfiguring the Cisco uBR7200 Series 2-2
Booting and Logging onto the Cisco uBR7200 Series 2-5
Setting Password Protection on the Cisco uBR7200 Series 2-5

Recovering Passwords on the Cisco uBR7200 Series 2-6
Configuring the Cisco uBR7200 Series Using AutoInstall 2-10
Autoinstall Requirements 2-10
Understanding AutoInstall 2-11
Preparing for the AutoInstall Process 2-11
Performing the AutoInstall Procedure 2-12
Setting Up the TFTP Server for Autoinstall 2-15
Setting Up the BOOTP or RARP Server for Autoinstall 2-16
Connecting the New Router to the Network 2-16
Configuring the Cisco uBR7200 Series Using the Setup Facility 2-17
Introduction to the Setup Facility 2-17
Configuring Global Parameters with the Setup Facility 2-18
Configuring Upstream Frequencies with the Setup Facility 2-21
Configuring Interfaces with the Setup Facility 2-22
Configuring the Cable Interface with the Extended Setup Facility 2-25
Identifying the Cable Interface Line Card 2-25
Configuring Global Parameters in Extended Setup 2-26
Configuring the Cisco uBR7200 Series Manually Using Configuration Mode 2-27
Saving Your Configuration Settings 2-29
Reviewing Your Settings and Configurations 2-29
Viewing Sample Configuration Files 2-29

CHAPTER 3 Configuring Cable Modem Interface Features 3-1
Configuring the Downstream Cable Modem Interface 3-2
Activating Downstream Cable Address Resolution Protocol Requests 3-2
Activating Downstream Ports 3-3
Setting the Integrated Upconverter 3-4
Assigning the Downstream Channel ID 3-5
Configuring Downstream Rate Limiting and Traffic Shaping 3-6
Setting the Downstream Helper Address 3-7
Setting the Downstream Interleave Depth 3-8
Setting the Downstream Modulation 3-8
Setting the Downstream MPEG Framing Format 3-9
Setting Downstream Traffic Shaping 3-10
Configuring the Upstream Cable Modem Interface 3-11
Activating Upstream Admission Control 3-12
Activating Upstream Differential Encoding 3-13
Activating Upstream Forward Error Correction 3-14
Activating the Upstream Ports 3-15

Activating Upstream Frequency Adjustment 3-15
Activating Upstream Power Adjustment 3-16
Activating the Upstream Scrambler 3-17
Activating Upstream Timing Adjustment 3-17
Configuring Upstream Rate Limiting and Traffic Shaping 3-18
Setting Upstream Backoff Values 3-19
Setting the Upstream Channel Width 3-21
Setting the Upstream Frequency 3-22
Setting the Upstream Input Power Level 3-24
Specifying Upstream Minislot Size 3-25
Setting Upstream Traffic Shaping 3-26
Configuring Optional Cable Modem Interface Features 3-28
Activating Host-to-Host Communication (Proxy ARP) 3-28
Activating Packet Intercept Capabilities 3-29
Configuring Cable Subinterfaces 3-29
Configuring and Monitoring Cable Interface Bundling 3-30
Configuring Payload Header Suppression and Restoration 3-33
Setting Optional IP Parameters (Broadcast and Multicast Echo) 3-33
Activating IP Multicast Echo 3-33
Activating IP Broadcast Echo 3-34

CHAPTER 4 Configuring DOCSIS Baseline Privacy Interface on the Cisco uBR7200 Series 4-1
Baseline Privacy Interface Overview 4-1
BPI Key Management 4-2
Differentiating Traffic Streams 4-3
CM Communication with BPI 4-3
Enabling DOCSIS BPI 4-3
DOCSIS 1.1 Baseline Privacy Interface Plus Overview 4-4

CHAPTER 5 Managing Cable Modems on the Hybrid Fiber-Coaxial Network 5-1
Activating Cable Modem Authentication 5-2
Activating Cable Modem Insertion Interval 5-3
Activating Cable Modem Upstream Address Verification 5-4
Clearing Cable Modem Counters 5-5
Clearing Cable Modem Reset 5-5
Configuring Cable Modem Registration Timeout 5-6
Configuring Dynamic Contention Algorithms (Cable Insertion Interval, Range, and Data Backoff) 5-6
cable insertion-interval Command Examples 5-6

Configuring the Dynamic Map Advance Algorithm 5-7
Configuring Maximum Hosts Attached to a Cable Modem 5-8
Configuring Per-Modem Filters 5-8
Configuring Sync Message Interval 5-9

CHAPTER 6 Configuring Basic Broadband Internet Access 6-1
Overview of Basic Broadband Internet Access 6-1
Recommended Basic Configuration for High-Speed Internet Access 6-2
Basic Internet Access Sample Configuration File 6-3

CHAPTER 7 Overview of the Cisco Network Registrar for the Cisco uBR7200 Series 7-1
Cisco Network Registrar Description 7-1
Cable Modem DHCP Response Fields 7-2
DOCSIS DHCP Fields 7-2
DHCP Relay Option (DOCSIS Option 82) 7-2
Overview of Scripts 7-3
Two-way Cable Modem Scripts 7-3
Telco Return Cable Modem Scripts 7-3
Placement of Scripts 7-3
Windows NT 7-3
Solaris 7-3
Activate Scripts in Cisco Network Registrar 7-4
Configuring the Cisco uBR7200 Series to Use Scripts 7-4
Configure the System Default Policy 7-5
Cable Modems 7-5
PCs 7-5
Create Selection Tag Scopes 7-5
General 7-5
Telco Return 7-6
Create Network Scopes 7-6
Create Policies for Class of Service or for Upgrading Cable Modem Cisco IOS Images 7-7
CNR Steps to Support Subinterfaces 7-7

CHAPTER 8 Troubleshooting the System 8-1
Understanding show Command Responses 8-2
Using a Headend Cable Modem to Verify Downstream Signals 8-6
Performing Amplitude Averaging 8-7

Enabling or Disabling Power Adjustment 8-7
Setting Downstream Test Signals 8-9
Configuring Unmodulated Test Signals 8-9
Configuring PRBS Test Signals 8-10
Verifying Test Signal Output 8-10
Pinging Unresponsive Cable Modems 8-10
Pinging a Cable Modem 8-10
Verifying the Ping 8-10
Using Cable Interface debug Commands 8-11
debug cable arp 8-11
debug cable error (for MAC Protocol Errors) 8-11
debug cable keyman (for Baseline Privacy Activity) 8-12
debug cable mac-messages 8-12
debug cable map 8-12
debug cable phy 8-12
debug cable privacy (for Baseline Privacy) 8-13
debug cable qos 8-13
debug cable range (for Ranging Messages) 8-13
debug cable receive (for Upstream Messages) 8-13
debug cable reg (for Modem Registration Requests) 8-14
debug cable reset (for Reset Messages) 8-14
debug cable specmgmt (for Spectrum Management) 8-14
debug cable startalloc (for Channel Allocations) 8-14
debug cable transmit (for CMTS Transmissions) 8-15
debug cable ucc (for Upstream Channel Change Messages) 8-15
debug cable ucd (for Upstream Channel Description Messages) 8-15

APPENDIX A Installing or Upgrading Cisco IOS Software A-1
Introduction A-1
Before You Begin A-1
Installing or Upgrading Cisco IOS Software A-2
Sample Output—Cisco uBR7200 Series Router A-3
Related Information A-3
Copying a System Image from One Device to Another A-4
Copying from Device to Device Inside the Same Router A-4
Copying from One Router to Another A-4

APPENDIX B Resolving Common Image Installation Problems B-1
Before You Begin B-1

Resolving Default Gateway Issues B-1
Troubleshooting Problems During Software Transfer B-3
Troubleshooting Problems by Verifying the Software Image B-5

APPENDIX C Viewing Sample Configuration Files C-1
Basic Internet Access Examples C-1
Virtual Private Network (VPN) Example C-9
IP Telephony Example C-12
Telco Return Example C-14

APPENDIX D Frequency Allocation for the Cisco uBR7200 Series Universal Broadband Routers D-1

APPENDIX E Configuration Register Information for the Cisco uBR7200 Series Universal Broadband Routers E-1
Configuration Bit Meanings E-1
Bits 0–3 E-2
Bit 6 E-3
Bit 7 E-3
Bit 8 E-3
Bit 10 and Bit 14 E-4
Bit 11 and Bit 12 E-4
Bit 13 E-5
Bit 15 E-5
Displaying the Configuration Register While Running Cisco IOS E-5
Displaying the Configuration Register While Running ROM Monitor E-6
Setting the Configuration Register While Running Cisco IOS E-6
Setting the Configuration Register While Running ROM Monitor E-7

INDEX

# Preface

This preface describes the objectives, intended audience, organization and terminology of this *Cisco uBR7200 Series Universal Broadband Router Software Configuration Guide.* The Cisco uBR7200 series CMTS and this guide support the following Cisco IOS release trains:

- 12.3 BC
- 12.2 BC
- 12.1 EC
- 12.0 SC

For additional supported Cisco IOS release trains, refer to *Cisco uBR7200 Series Software Release Notes* on Cisco.com.

## Document Revision History

The Document Revision History table below records technical changes to this document.

*Table 1 Document Revision History*

| Document Revision | Date | Change Summary |
|---|---|---|
| OL-2239-04 | September 30, 2005 | Incorporated new features and enhancements introduced in Cisco IOS Release 12.3(13a)BC. Added Document Revision History table. |

## Document Objectives

This guide describes configuring, maintaining, and troubleshooting the Cisco uBR7200 series universal broadband routers: the Cisco uBR7223, Cisco uBR7246, and Cisco uBR7246 VXR. Cisco's Cable Modem Termination System (CMTS) solutions allow cable companies, Internet service providers (ISPs), and others to allocate channel capacity for Internet access, Virtual Private Network (VPN), and Voice over IP (VoIP) services using a broadband radio frequency (RF) cable plant.

The Cisco uBR7200 series universal broadband routers sustain downstream and upstream traffic to and from two-way Data Over Cable Service Interface Specification (DOCSIS)-based cable modems (CMs) that support 6 MHz National Television Systems Committee (NTSC) operations. For NTSC cable plants not upgraded for full two-way operations, the routers also support DOCSIS-compliant telco-return CMs. For international cable companies using 8 MHz channel widths, the Cisco uBR7200 series equipment supports Phase Alternating Line (PAL) and Systeme Electronique Couleur Avec Memoire (SECAM) channel plans to operate with EuroDOCSIS-based CMs and set top box (STB) units with integrated EuroDOCSIS modems.

# Audience

This guide is intended for system administrators and support engineers who configure and maintain the Cisco uBR7200 series. Many different delivery models exist for Cisco uBR7200 series equipment:

- In smaller networks, a single service provider manages all equipment and infrastructure.
- In larger networks, multiple service operators (MSOs) and ISPs share responsibility for provisioning and managing the cable plant and IP network.

The MSO and ISP divide responsibilities according to the service model. In some cases, the MSO maintains and operates the cable plant and attached CMs and STBs, whereas the ISP owns, operates, and maintains the regional network and IP infrastructure beyond the cable distribution hub. In other cases, the CMTS and RF customer premises equipment (CPE) are viewed as part of the networking infrastructure, and the ISP maintains control for provisioning and managing DOCSIS functionality.

Note This guide considers the MSO and ISP as a single service principle with responsibility to provision and manage DOCSIS-based cable modems and set-top boxes (STBs). This guide assumes that administrators are familiar with Cisco uBR7200 series hardware, DOCSIS or EuroDOCSIS requirements, and networking.

# Document Organization

This guide focuses on configuration of Cisco IOS software for the Cisco uBR7200 series. Table 2 summarizes the chapters and procedures in this guide.

*Table 2 Guide Contents and Organization*

| Title | Description |
|---|---|
| Chapter 1, “Overview of Cisco uBR7200 Series Software” | Acquaints you with the supported Cisco IOS features and configuration. |
| Chapter 2, “Configuring the Cable Modem Termination System for the First Time” | Provides instructions to make basic configurations to the Cisco uBR7200 series cable modem termination system (CMTS) using AutoInstall, the Setup facility, Extended Setup, or manual configuration mode. Includes sample Cisco uBR7200 series software configurations.<br>Note Complete the configurations in this chapter prior to attempting additional configurations later in this guide or elsewhere. |
| Chapter 3, “Configuring Cable Modem Interface Features” | Provides instructions for required cable modem interface configurations for upstream and downstream interfaces. |
| Chapter 4, “Configuring DOCSIS Baseline Privacy Interface on the Cisco uBR7200 Series” | Provides an overview of DOCSIS 1.0 Baseline Privacy Interface (BPI), instructions for enabling BPI, and an introduction to DOCSIS 1.1 BPI+ features. |
| Chapter 5, “Managing Cable Modems on the Hybrid Fiber-Coaxial Network” | After completing upstream and downstream cable modem interface configurations, this chapter provides a number of procedures that you can implement in order to manage operations of your cable modems in the hybrid fiber-coaxial network. |
| Chapter 6, “Configuring Basic Broadband Internet Access” | Provides a recommended basic configuration for high-speed Internet access and a basic Internet access sample configuration file. |

*Table 2 Guide Contents and Organization (continued)*

| Title | Description |
|---|---|
| Chapter 7, “Overview of the Cisco Network Registrar for the Cisco uBR7200 Series” | Supplements the Cisco Network Registrar (CNR) documentation by providing additional cable-specific instructions that are pertinent to the Cisco uBR7200 series and CMTS management. |
| Chapter 8, “Troubleshooting the System” | Provides troubleshooting instructions for the configuration of the Cisco uBR7200 series CMTS. |
| Appendix A, “Installing or Upgrading Cisco IOS Software” | Explains how to install Cisco IOS software onto "Run from RAM" Cisco routers using a TFTP server or remote copy protocol (rcp) server application. |
| Appendix B, “Resolving Common Image Installation Problems” | Explains the resolution to common installation problems when installing images using TFTP or an rcp server. |
| Appendix C, “Viewing Sample Configuration Files” | Provides examples of Cisco uBR7200 series universal broadband router configuration files. |
| Appendix D, “Frequency Allocation for the Cisco uBR7200 Series Universal Broadband Routers” | Provides information on NTSC 6-MHz, Phase Alternating Line (PAL) and Systeme Electronique Couleur Avec Memoire (SECAM) 8-MHz channel bands. |
| Appendix E, “Configuration Register Information for the Cisco uBR7200 Series Universal Broadband Routers” | Provides information about the functions and configuration of bits in the Cisco IOS Software Configuration Register. |
| Index | Index for the entire manual. |

# Conventions

This guide uses the following conventions for command syntax descriptions and textual emphasis:

*Table 3 Command Syntax and Emphasis Conventions*

| Convention | Description |
|---|---|
| **boldface** font | Commands and keywords are in **boldface**. |
| *italic* font | Arguments for which you supply values are in *italics*. |
| [ ] | Elements in square brackets are optional. |
| {*x* \| *y* \| *z*} | Alternative, mutually exclusive, keywords are grouped in braces and separated by vertical bars. |
| [*x* \| *y* \| *z*] | Optional alternative keywords are grouped in brackets and separated by vertical bars. |
| string | A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks. |
| `screen` font | Terminal sessions and information the system displays are in `screen` font. |
| **`boldface screen`** font | Information you must enter is in **`boldface screen`** font. |
| *`italic screen`* font | Arguments for which you supply values are in *`italic screen`* font. |
| ^ | The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key. |

*Table 3 Command Syntax and Emphasis Conventions (continued)*

| Convention | Description |
|---|---|
| < > | Nonprinting characters, such as passwords, are in angle brackets in contexts where italics are not available. |
| [ ] | Default responses to system prompts are in square brackets. |
| !, # | An exclamation point ( ! ) or a pound sign ( # ) at the beginning of a line of code indicates a comment line. |

Note This symbol means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Tip This symbol means *the following are useful tips.*

Timesaver This symbol means *the described action saves time*. You can save time by performing the action described in the paragraph.

Caution This symbol means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

# Terms and Acronyms

A complete list of terms and acronyms is available in the *Internetworking Terms and Acronyms* guide, available on the Documentation CD-ROM and at http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/.

To fully understand the content of this guide, you should be familiar with the following terms and acronyms.

- A/D—analog to digital (conversion)
- ABR—available bit rate
- AAL5—ATM adaptation layer 5
- AGC—automatic gain control
- AM-VSB—Amplitude Modulation - Vestigial Side Band (Modulation scheme)
- ASIC—Application Specific Integrated Circuit
- AWG—American wire gauge
- BGP—Border Gateway Protocol
- BPI—Baseline Privacy Interface
- CATV—cable television
- CM—cable modem
- CMTS—cable modem termination system (headend)

- CoS—class of service
- CPE—customer premises equipment
- CPR—Centralized Priority Reservation
- CRC—cyclic redundancy check
- CSU—channel service unit
- CTS—Clear To Send
- D/A—digital to analog (conversion)
- DAVIC —Digital Audio-Visual Council
- DCD—Data Carrier Detect
- DCE—data communications equipment
- DDS—Direct Digital Synthesis
- DES—Data Encryption Standard
- DHCP—Dynamic Host Configuration Protocol
- DOCSIS—Data-over-Cable Service Interface Specification
- DVB—Digital Video Broadcasting
- DIMM—dual in-line memory module
- DSR—data set ready
- DSU—data service unit
- DTE—data terminal equipment
- DTR—data terminal ready
- ESP—Electronic Systems Products
- EMC—electromagnetic compliance
- EMI—electromagnetic interference
- ESD—electrostatic discharge
- EuroDOCSIS—European DOCSIS (Data-over-Cable Service Interface Specification)
- FCS—Frame Check Sequence; First Customer Shipment
- FDR—Final Design Review
- FEC—Forward Error Correction
- FRU—field-replaceable unit (router components that do not require replacement by a service provider certified by Cisco)
- FTP—foil twisted-pair
- HCCP—Hot Standby CMTS-to-CMTS Protocol
- HDLC—High-Level Data Link Control
- HEAD—Head-end Modulator and Demodulator
- HEM—Head End Modem
- HFC—Hybrid Fiber Coax
- HOME—Subscriber Unit
- HS—Head-end Shelf
- HSRP—Hot-Standby Router Protocol
- IP—Internet Protocol
- IPSec—IP Security Protocol
- ISL—Inter-Switch Link protocol
- ISS—Instruction Set Simulator

- Kbps—kilo-bits per second
- LAN—local area network
- LCN—logical channel number
- LED—light emitting diode
- LLC—logical link control
- MAC—Media Access Control
- MB—megabyte
- Mbps—mega-bits per second
- MM—multimode
- MODEM—modulator/demodulator
- MPEG-2—Moving Picture Experts Group (Specification 2)
- MPEG-2-TS—MPEG-2 Transport Stream
- MSN—manufacturer serial number
- MSO—multiple systems operator
- NIU/STB—network interface unit/set-top box
- nrt-VBR—non-real-time variable bit rate
- NTSC—National Television Standards Committee
- NVRAM—nonvolatile random-access memory
- OAM AIS—Operation, Administration, and Maintenance alarm indication signal
- OAM&P—Operations, Administration, Maintenance and Provisioning
- OC3—Optical Carrier Level 3
- OIR—online insertion and removal
- PCI—Peripheral Component Interconnect
- PCMCIA—Personal Computer Memory Card International Association
- PDD—Project Design Document
- PHY—Physical Layer Interface
- PID—Packet Identifier
- PLL—Phase Locked Loop
- PPP—Point-to-Point Protocol
- QAM—Quadrature Amplitude Modulation
- QoS—quality of service
- QPSK—Quadrature Phase Shift Keying
- rcp—remote copy protocol
- RFI—radio frequency interference
- RIP—Routing Information Protocol
- RISC—Reduced Instruction Set Computer
- RTP—Real-Time Transport Protocol
- RTS—Request To Send
- SDRAM—synchronous dynamic random-access memory
- SIMM—single in-line memory module
- SM—Subscriber Modem or Spectrum Manager
- SMI—single-mode intermediate reach

- SNMP—Simple Network Management Protocol
- SU—Subscriber Unit
- TCP/IP—Transmission Control Protocol/Internet Protocol
- TDE/C—Transmit Data Encoder/Controller
- TDM—time-division multiplexing
- TDMA—Time Division Multiple Access
- TFTP—Trivial File Transfer Protocol
- UBR—unspecified bit rate
- UDP—User Datagram Protocol
- UNI—User-Network Interface
- UTOPIA—Universal Test and Operation Physical Interface for ATM
- UTP—unshielded twisted-pair
- VC—virtual circuit
- VCI—Virtual Channel Identifier
- VCPU—Virtual CPU
- VP—Virtual Path
- VPI—Virtual Path Identifier
- VPN—Virtual Private Network

# Related Documentation

## Cisco uBR7200 Series Documentation

The procedures in this guide assume that site preparation and hardware setup are complete. Refer to the documentation page for *Cisco uBR7200 Series Universal Broadband Routers* for these and additional document links:

| Document Title | Online Location |
|---|---|
| *Release Notes for the Cisco uBR7200 Series* (multiple release trains) | http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200rn/index.htm |
| *Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide* | http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cr72hig/index.htm |
| *Cisco uBR7200 Series — Universal Broadband Router Product Overview* | http://www.cisco.com/univercd/cc/td/doc/pcat/ub7200.htm |
| *Cisco uBR7200 Series Software Features* | http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200sw/index.htm |

Note If the hypertext link to any external document does not operate, you can access the desired document by typing or pasting the full document title in the **Search** field of the Cisco.com home page. Click **Go**.

- For information about installing and replacing field-replaceable units (FRUs), such as memory, on Cisco uBR7200 series routers, refer to the document that ships with each FRU.
- For information on the modular port adapter installed in your router (if present), refer to the individual documents that ship with each port adapter.
- For international agency compliance, safety, and statutory information for WAN interfaces for Cisco uBR7200 series routers, refer to the *Regulatory Compliance and Safety Information* document that shipped with your router.

# Cisco Cable Modem Termination System Reference Documentation

| Document Title | Online Location |
|---|---|
| *Cable DOCSIS 1.1 FAQs* | http://www.cisco.com/warp/public/109/cable_faq_docsis11.html |
| *Cisco Cable Modem Termination System Feature Guide* | http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ |
| *Cisco Broadband Cable Command Reference Guide* | http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/ |
| *Cisco IOS Multiservice Applications Configuration Guide:*<br>• *Configuring Headend Broadband Access Router Features*<br>• *Configuring Subscriber-End Broadband Access Router Features* | http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/multi_c/mcprt3/index.htm |
| *DOCSIS 1.1 for the Cisco uBR7200 Series Universal Broadband Routers* | http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200sw/index.htm |

# Related Cisco IOS Release Documentation

For detailed Cisco IOS software configuration information and support, refer to the configuration and command reference publications on these web pages:

- *Cisco IOS Release 12.1 Documentation*
- *Cisco IOS Release 12.2 Documentation*
- To query Cisco IOS releases according to feature or release number, refer to the *Cisco IOS Feature Navigator* (Cisco.com login ID and password required).

# Additional Documentation Resources

## World Wide Web

You can access the most current Cisco documentation on the World Wide Web at http://www.cisco.com.

## Translated Documentation

Translated documentation is available at http://www.cisco.com/public/countries_languages.shtml.

## Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

## Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace at http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store at http://www.cisco.com/go/subscription
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Feedback** at the top of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

# Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web site.

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support

- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to http://www.cisco.com.

# Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

## Cisco TAC Web Site

The Cisco TAC Web site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web site, refer to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web site. The Cisco TAC Web site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, refer to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web site.

## Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, refer to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

# Overview of Cisco uBR7200 Series Software

The Cisco uBR7200 series uses Cisco IOS® software to offer enhanced stability, features, performance and investment protection. This chapter summarizes system and software features of the Cisco uBR7200 series Cable Modem Termination System (CMTS). This chapter contains the following sections:

| Section | Purpose |
|---|---|
| "Cisco IOS Releases and Images for the Cisco uBR7200 Series," page 2 | Describes the supported Cisco IOS release trains, associated features, and latest Cisco IOS images for each recently supported train.<br>One early step in CMTS feature configuration is to verify your Cisco IOS release train, the associated image and feature set. This section guides you in determining such information. |
| "Cisco uBR7200 Series Chassis Overview," page 8 | Describes the Cisco uBR7200 series routers, and their supported hardware features and interoperability. |
| "Cisco uBR7200 Series Router Configuration Overview," page 15 | Provides an overview of the hardware and interfaces that typically require configuration through Cisco IOS software. |
| "Supported Software Features for the Cisco uBR7200 Series," page 22 | Describes the features and configuration utilities that are available on the Cisco uBR7200 series. |
| "DOCSIS and CMTS Interoperability," page 137 | Provides an overview of DOCSIS NTSC and EuroDOCSIS cable plants, DOCSIS-compliant signals, and traffic engineering. |

# Cisco IOS Releases and Images for the Cisco uBR7200 Series

This section describes the supported releases, latest images, memory requirements, and major software features for the following Cisco IOS software:

- Determining Your Cisco IOS Software Release
- Upgrading to a New Software Release
- 12.3 BC Release Train Images and Requirements
- 12.2 BC Release Train Images and Requirements
- 12.2 CX Images and Requirements
- 12.1 EC Images and Requirements

To configure the CMTS for the first time, refer to Chapter 2, "Configuring the Cable Modem Termination System for the First Time."

For additional release information, refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200rn/index.htm

## Determining Your Cisco IOS Software Release

To determine the version of Cisco IOS software running on the Cisco uBR7200 series universal broadband router, log in to the router and enter the **show version** command in User or privileged EXEC mode.

```
Router> show version

Cisco Internetwork Operating System Software
IOS (tm) Cisco IOS 12.2 BC Software (ubr7200-is-mz), Version Cisco IOS Release 12.2(4)BC1,
RELEASE SOFTWARE
```

Note Your display may vary according to your release and image.

## Upgrading to a New Software Release

An upgrade is an order placed for a Cisco IOS feature set that contains more functionality than the feature set that you are replacing. An upgrade is not an "update." An update consists of installing a more recent version of the *same* feature set.

- **Exception**—If a feature set has been made obsolete, the next closest feature set on a more recent release is considered an update.

For general information about upgrading to a new software release, refer to the *Cisco IOS Upgrade Ordering Instructions* on Cisco.com. Also refer to Appendix A, "Installing or Upgrading Cisco IOS Software."

# 12.3 BC Release Train Images and Requirements

The Cisco 12.3 BC release train is the latest Cisco IOS release train to support the Cisco uBR7200 Series, and emphasizes additional features and performance specifically for the Cisco uBR7246VXR universal broadband router.

Table 1-2 displays the memory recommendations of the Cisco IOS feature sets for the Cisco uBR7200 series universal broadband routers for Cisco IOS Release 12.3(9a)BC. Cisco uBR7200 series routers are only available with a 48 MB or 128 MB of Flash disk memory on the I/O Controller cards. The UBR7200-NPE-G1 uses compact Flash disk only.

Note Flash disks, an alternative to linear Flash memory, are Flash memory-based devices that can be used as file storage media in the PCMCIA card slots of the I/O Controllers. Each I/O Controller has two PCMCIA slots and can be configured with up to 256 MB of Flash disk memory.

*Table 1 Memory Recommendations for the Cisco uBR7200 Series Routers, Cisco IOS Release 12.3(9a)BC Feature Sets*

| Feature Set | Software Image | Recommended Flash Memory | Recommended DRAM Memory | Runs From |
|---|---|---|---|---|
| Two-Way Data/VoIP Images | | | | |
| DOCSIS Two-Way | ubr7200-p-mz | 32 MB Flash | 256 MB DRAM | RAM |
| DOCSIS Two-Way IP Plus | ubr7200-is-mz | 32 MB Flash | 256 MB DRAM | RAM |
| DOCSIS Two-Way with BPI | ubr7200-k8p-mz | 32 MB Flash | 256 MB DRAM | RAM |
| DOCSIS Two-Way IP Plus with BPI | ubr7200-ik8s-mz | 32 MB Flash | 256 MB DRAM | RAM |
| DOCSIS Two-Way 3DES | ubr7200-k9p-mz | 32 MB Flash | 256 MB DRAM | RAM |
| DOCSIS Two-Way 3DES IP Plus | ubr7200-ik9s-mz | 32 MB Flash | 256 MB DRAM | RAM |
| Boot Image | | | | |
| UBR7200 Boot Image | ubr7200-kboot-mz | None | None | — |
| UBR7200 Boot Image | ubr7200-boot-mz | None | None | — |

The image subset legend for Table 1-2 is as follows:

- i = IP routing, MPLS-VPN support, and non-cable interface bridging, including Network Address Translation (NAT)
- k8 = DOCSIS Baseline Privacy
- p = IP routing with Intermediate System-to-Intermediate System (IS-IS) and Border Gateway Protocol (BGP); MPLS-VPN support; no bridging and no NAT
- s = “Plus” features: NAT and Inter-Switch Link (ISL)
- k9 = 3DES level of encryption

Note All images support all of the hardware listed in the “Supported Hardware on the Cisco uBR7200 Series” section on page 1-11, unless otherwise indicated.

Note A Cisco uBR7200 series router requires 256 MB of DRAM memory on the NPE processor card when HCCP redundancy is configured and the router is supporting more than 3,000 cable modems. Using less memory in these conditions results in temporary out-of-memory situations and incomplete synchronization between the Working and Protect interfaces.

# 12.2 BC Release Train Images and Requirements

Note Cisco IOS release 12.2(4)BC1 offers certified DOCSIS 1.1 support on the Cisco uBR7246 VXR router.

The 12.2 BC train is an interim release train that provides certified DOCSIS 1.1 two-way support on the Cisco uBR7246 VXR universal broadband router, along with support for selected new features. The latest release in this train, Cisco IOS Release 12.2(4)BC1, provides a migration path from the earlier Cisco IOS 12.2 XF releases, which included a subset of the features supported in these Cisco IOS release trains:

- Cisco IOS Release 12.0 SC
- Cisco IOS Release 12.1 EC
- Cisco IOS Release 12.1 CX1

Table 1-2 displays the memory recommendations of the Cisco IOS feature sets for the Cisco uBR7200 series universal broadband routers for Cisco IOS Release 12.2(15)BC1 and 12.2(15)BC2a. Cisco uBR7200 series routers are available with 48 MB or 128 MB of Flash disk memory on the I/O Controller cards. The UBR7200-NPE-G1 uses compact Flash disk only.

Note Flash disks, an alternative to linear Flash memory, are Flash memory-based devices that can be used as file storage media in the PCMCIA card slots of the I/O Controllers. Each I/O Controller has two PCMCIA slots and can be configured with up to 256 MB of Flash disk memory.

Note Cisco IOS release 12.2(4)BC1and later BC releases offer certified DOCSIS 1.1 support on the Cisco uBR7246 VXR router.

*Table 1-2 Memory Recommendations for the Cisco uBR7200 Series Routers, Cisco IOS Release 12.2(15)BC1 and 12.2(15)BC2a Feature Sets*

| Feature Set | Software Image | Recommended Flash Memory | Recommended DRAM Memory | Runs From |
|---|---|---|---|---|
| Two-Way Data/VoIP Images | | | | |
| DOCSIS Two-Way | ubr7200-p-mz | 16 MB Flash<br>32 MB Flash[1] | 128 MB DRAM | RAM |
| DOCSIS Two-Way IP Plus | ubr7200-is-mz | 16 MB Flash<br>32 MB Flash[1] | 128 MB DRAM | RAM |
| DOCSIS Two-Way with BPI | ubr7200-k8p-mz | 16 MB Flash<br>32 MB Flash[1] | 128 MB DRAM | RAM |
| DOCSIS Two-Way IP Plus with BPI | ubr7200-ik8s-mz | 16 MB Flash<br>32 MB Flash[1] | 128 MB DRAM | RAM |
| DOCSIS Two-Way 3DES | ubr7200-k9p-mz | 16 MB Flash<br>32 MB Flash[1] | 128 MB DRAM | RAM |
| DOCSIS Two-Way 3DES IP Plus | ubr7200-ik9s-mz | 16 MB Flash<br>32 MB Flash[1] | 128 MB DRAM | RAM |
| **Boot Image** | | | | |
| UBR7200 Boot Image | ubr7200-kboot-mz | None | None | — |
| UBR7200 Boot Image | ubr7200-boot-mz | None | None | — |

1. 32 MB of Flash is required for Cisco IOS Release 12.2(15)BC2a and later releases in the Cisco IOS BC train.

The image subset legend for Table 1-2 is as follows:

- i = IP routing, MPLS-VPN support, and non-cable interface bridging, including Network Address Translation (NAT)
- k8 = DOCSIS Baseline Privacy
- p = IP routing with Intermediate System-to-Intermediate System (IS-IS) and Border Gateway Protocol (BGP); MPLS-VPN support; no bridging and no NAT
- s = "Plus" features: NAT and Inter-Switch Link (ISL)
- k9 = 3DES level of encryption

Note All images support all of the hardware listed in the "Supported Hardware on the Cisco uBR7200 Series" section on page 1-11, unless otherwise indicated.

Note A Cisco uBR7200 series router requires 256 MB of DRAM memory on the NPE processor card when HCCP redundancy is configured and the router is supporting more than 3,000 cable modems. Using less memory in these conditions results in temporary out-of-memory situations and incomplete synchronization between the Working and Protect interfaces.

## 12.2 CX Images and Requirements

The 12.2 CX releases are based on Cisco IOS Release 12.2(15)BC1, which is a child of Cisco IOS Release 12.2(15)T. The 12.2 BC train is an interim release train that provides DOCSIS 1.1 two-way support, along with fixes for software caveats and support for selected new features.

The latest image in the 12.2 CX release train, Cisco IOS Release 12.2(15)CX1, provides two different boot images for the Cisco uBR7200 series routers:

- ubr7200-kboot-mz.122-15.CX.bin

  The "kboot" version of the boot image is a new version of the boot image software that can run only on the Cisco uBR7200-NPE-G1 processor and the UBR7200-I/O-2FE/E I/O controller, because it is too large to load on the other I/O controllers. This image contains support for almost all supported port adapters, allowing the Cisco uBR7246VXR router to boot over almost any type of WAN interface.

- ubr7200-boot-mz.122-15.CX.bin

  The "boot" version of the boot image is small enough to be loaded on I/O controllers with 4MB of Flash memory, but it supports only Ethernet, FastEthernet, Gigabit Ethernet, OC POS, and a limited number of ATM port adapters. If you are using a serial port adapter or most ATM port adapters, you will not be able to boot over the WAN interface.

This difference in boot images affects only the ability of the Cisco uBR7246VXR router to boot over the WAN interface. When the router has successfully loaded the Cisco IOS software, it has connectivity over all of the port adapters that this particular version of Cisco IOS software supports.

Table 1-3 displays the memory recommendations of the Cisco IOS feature sets for the Cisco uBR7200 series universal broadband routers for Cisco IOS Release 12.2(15)CX1. Cisco uBR7200 series routers are only available with a 48 MB or 128 MB of Flash disk memory on the I/O Controller cards. The UBR7200-NPE-G1 uses only compact Flash disk.

Flash disks, an alternative to linear Flash memory, are Flash memory-based devices that can be used as file storage media in the PCMCIA card slots of the I/O Controllers. Each I/O Controller has two PCMCIA slots and can be configured with up to 256 MB of Flash disk memory.

*Table 1-3 Memory Recommendations for the Cisco uBR7200 Series Routers, Cisco Release 12.2(15)CX1 Feature Sets*

| Feature Set | Software Image | Recommended Flash Disk Memory | Recommended DRAM Memory | Runs From |
|---|---|---|---|---|
| Two-Way Data/VoIP Images | | | | |
| DOCSIS Two-Way | ubr7200-p-mz | 48 MB Flash | 128 MB DRAM | RAM |
| DOCSIS Two-Way IP Plus | ubr7200-is-mz | 48 MB Flash | 128 MB DRAM | RAM |
| DOCSIS Two-Way with BPI | ubr7200-k8p-mz | 48 MB Flash | 128 MB DRAM | RAM |
| DOCSIS Two-Way IP Plus with BPI | ubr7200-ik8s-mz | 48 MB Flash | 128 MB DRAM | RAM |
| DOCSIS Two-Way 3DES | ubr7200-k9p-mz | 48 MB Flash | 128 MB DRAM | |
| DOCSIS Two-Way 3DES IP Plus | ubr7200-ik9s-mz | 48 MB Flash | 128 MB DRAM | |

The image subset legend for Table 1-3 is as follows:

- i = IP routing, MPLS-VPN support, and non-cable interface bridging, including Network Address Translation (NAT)
- k8 = DOCSIS Baseline Privacy
- p = IP routing with Intermediate System-to-Intermediate System (IS-IS) and Border Gateway Protocol (BGP); MPLS-VPN support; no bridging and no NAT
- s = "Plus" features: NAT and Inter-Switch Link (ISL)
- k9 = 3DES level of encryption

# 12.1 EC Images and Requirements

The 12.1 EC train is the Cisco cable-specific early deployment release train that introduces several new feature sets, support for the Cisco uBR-MC28C cable interface line card, and several new software features.

Table 4 displays the memory recommendations of the Cisco IOS feature sets for the Cisco uBR7200 series universal broadband routers for the latest Cisco IOS Release 12.1(20)EC1. Cisco uBR7200 series routers support a 16-MB or 20-MB Type II PCMCIA Flash memory card.

*Table 4 Memory Recommendations for the Cisco uBR7200 Series Routers, Cisco Release 12.1(20)EC1 Feature Sets*

| Feature Set | Software Image | Recommended Flash Memory | Recommended DRAM Memory | Runs From |
|---|---|---|---|---|
| Two-Way Data/VoIP Images | | | | |
| DOCSIS Two-Way | ubr7200-p-mz | 16 MB Flash | 128 MB DRAM | RAM |
| DOCSIS Two-Way IP Plus | ubr7200-is-mz | 16 MB Flash | 128 MB DRAM | RAM |
| DOCSIS Two-Way with BPI | ubr7200-k1p-mz | 16 MB Flash | 128 MB DRAM | RAM |
| DOCSIS Two-Way IP Plus with BPI | ubr7200-ik1s-mz | 16 MB Flash | 128 MB DRAM | RAM |
| Telco-Return Images | | | | |
| DOCSIS IP Plus Telco Return | ubr7200-ist-mz | 16 MB Flash | 128 MB DRAM | RAM |
| DOCSIS IP Plus Telco Return with BPI | ubr7200-ik1st-mz | 16 MB Flash | 128 MB DRAM | RAM |
| Boot Image | | | | |
| UBR7200 Boot Image[1] | ubr7200-boot-mz | None | None | — |

1. The 12.1 EC UBR7200 boot image is provided for the IUBR7200-I/O-2FE/E input/output controller, which must use the Cisco IOS 12.1(10)EC1 or later 12.1 EC release boot image. This image cannot be used on any other I/O controllers.

The image subset legend for Table 4 is as follows:

- i = IP routing, MPLS-VPN support, and non-cable interface bridging, including Network Address Translation (NAT)
- k1 = DOCSIS Baseline Privacy and MPLS-VPN support
- p = IP routing with Intermediate System-to-Intermediate System (IS-IS) and Border Gateway Protocol (BGP); MPLS-VPN support; no bridging and no NAT
- s = “Plus” features: NAT and Inter-Switch Link (ISL)
- t = DOCSIS telco return

Note All images support all of the hardware listed in the section “Supported Hardware on the Cisco uBR7200 Series” section on page 1-11, unless otherwise indicated.

# Cisco uBR7200 Series Chassis Overview

The Cisco uBR7200 series universal broadband routers allow high-speed data services to be packaged similar to cable TV service or video fare. Cisco uBR7200 Series equipment supports data and digitized voice connectivity between Internet Protocol (IP) hosts and connected subscribers using a bidirectional cable TV and IP backbone.

Note For 6 MHz National Television Systems Committee (NTSC) cable plants not fully upgraded to two-way transmission, the equipment works with dial-up access products to support upstream traffic from Data-over-Cable Service Interface Specification (DOCSIS)-based telco-return cable interfaces.

For international cable plants that use 8-MHz Phase Alternating Line (PAL) or Systeme Electronique Couleur Avec Memoire (SECAM) channel plans, Cisco uBR7200 Series equipment supports bidirectional transfer of traffic between the Cable Modem Termination System (CMTS) and EuroDOCSIS-based CMs or set top box (STB) units with integrated EuroDOCSIS modems.

Cable companies and Internet service providers (ISPs) can allocate radio frequency (RF) channel capacity for Internet access, Virtual Private Network (VPN), or Voice over IP (VoIP) services using a hybrid fiber/coax (HFC) or all-coax cable plant. Cisco currently provides three router-based DOCSIS CMTS solutions that offer a wider feature set and better manageability than bridge-based systems.

- **Cisco uBR7246 VXR Universal Broadband Router**—Supports higher density and broad media configurations; the chassis contains up to two single-width IP backbone interfaces, up to four cable TV RF interfaces, up to two power supplies, an optional clock interface that enables the router to synchronize to an external timing reference, a faster processor, and higher bus bandwidth.
- **Cisco uBR7246 Universal Broadband Router**—Supports large cable installations; the chassis contains up to two single-width IP backbone interfaces, up to four cable TV RF interfaces, and up to two power supplies.
- **Cisco uBR7223 Universal Broadband Router**—Supports small-to-medium cable installations; the chassis contains one single-width IP backbone interface and up to two cable TV RF interfaces.

Note This guide focuses on Cisco uBR7200 Series software. For detailed descriptions of Cisco uBR7200 Series chassis and components, refer to the *Cisco uBR7200 Series Hardware Installation Guide* and appropriate field replaceable unit (FRU) documents on Cisco.com.

Cisco cable interface line cards serve as the RF cable TV interfaces, supporting downstream and upstream signal combining and splitting arrangements. The cards currently require external upconverters to connect to the cable system. Cisco port adapters connect to the IP backbone and external networks. Your cable plant, combined with your planned and installed subscriber base, service offering, and external network connections, determine the Cisco uBR7200 Series chassis, cable interface line cards, port adapters, and other components you use.

Data is modulated or demodulated using either of the following two methods:

- Downstream 6 MHz channels in the 54-to-860 MHz range with upstream ranges of 5 to 42 MHz. Cisco MC11 FPGA, MC11C, MC12C, MC14C, MC16B, MC16C, and MC16S cable interface line cards support NTSC channel operation, using standard (STD), Harmonic Related Carrier (HRC), or Incremental Related Carrier (IRC) frequency plans conforming to EIA-S542.

  NTSC uses a 6 MHz-wide modulated signal with an interlaced format of 25 frames per second and 525 lines per frame. NTSC is compatible with CCIR Standard M. PAL, used in West Germany, England, Holland, Australia, and several other countries.

Note Cisco 6 MHz products can be used in 8 MHz cable plants. The products, however, operate at a maximum downstream bandwidth of 27 Mbps, ignoring 2 MHz of available channel width, and limiting upstream channel choices to the range below 42 MHz.

- Downstream 8 MHz channels in the 85-to-860 MHz range with an upstream range of 5 to 65 MHz. The Cisco MC16E cable interface line card supports PAL and SECAM channel plans using an 8 MHz modulated signal.

  PAL uses a 625-line scan picture delivered at 25 frames per second where the color carrier phase definition changes in alternate scan lines. SECAM uses an 819 line scan picture that provides better resolution than PAL's 625-line and NTSC's 525-line.

  The MC16E uses the EuroDOCSIS J.112 (Annex A) standard, CableLabs ECR RFI-R-98036, which is similar to the Digital Audio Video Council/Digital Video Broadcast (DAVIC/DVB) ITU J.83 Annex A physical layer. Cable companies can support data, voice, and video services with DOCSIS-based CMs or set top boxes (STBs) that contain integrated EuroDOCSIS modems.

Caution The MC16E supports only Annex A operation and should not be used in production cable plants that support a 6 MHz channel plan.

Note The difference between DOCSIS and EuroDOCSIS is at the physical layer. EuroDOCSIS support requires the Cisco MC16E cable interface line card, appropriate upconverters that support an 8 MHz PAL or SECAM channel plan, appropriate diplex filters, and EuroDOCSIS-based CMs or STBs.

The DOCSIS Radio Frequency (RF) specification defines the RF communication paths between the CMTS and CMs (or CMs in STBs). The DOCSIS RF specification defines the physical, link, and network layer aspects of the communication interfaces. It includes specifications for power level, frequency, modulation, coding, multiplexing, and contention control. Cisco offers products that support all DOCSIS error correction encoding and modulation types and formats, and that support DOCSIS Annex B or EuroDOCSIS Annex A operations.

## Cisco uBR7200 Series Universal Broadband Routers

The Cisco uBR7200 series universal broadband routers are based on the Data-over-Cable Service Interface Specification (DOCSIS) standards. Each is designed to be installed at a cable operator's headend facility or distribution hub and to function as the cable modem termination system (CMTS) for subscriber-end devices such as the Cisco uBR905 and Cisco uBR925 cable access routers, and other DOCSIS-compliant CMs and set-top boxes (STBs).

Cisco uBR7200 series universal broadband routers allow two-way transmission of digital data and Voice over IP (VoIP) traffic over a hybrid fiber-coaxial (HFC) network. For cable plants not fully upgraded to support two-way cable transmission, the routers support DOCSIS-compliant telco return, where the cable modem's return path to the CMTS uses a dial-up telephone line connection instead of an upstream channel over the coaxial cable. The telco-return delivery mechanism enables cable operators to accelerate deployment of high-speed data services before the cable systems are upgraded to two-way plants.

The Cisco uBR7200 series routers support IP routing with a wide variety of protocols and combinations of Ethernet, Fast Ethernet, Gigabit Ethernet, serial, High-Speed Serial Interface (HSSI), Packet over SONET (POS) OC-3 and OC-12c, and Asynchronous Transfer Mode (ATM) media.

## Cisco uBR7246 VXR Universal Broadband Router

The Cisco uBR7246VXR offers an industry-proven CMTS and carrier-class router in a scalable platform with a high-performance network processing engine to support data, voice, and video services for medium to large network installations.

The Cisco uBR7246 VXR provides the following major hardware features:

- High-performance network processing engine or network services engine
- I/O controller
- Up to two network interface port adapters
- Up to four cable interface line cards
- Up to two removable power supplies providing load-sharing and redundancy capabilities
- Two Personal Computer Memory Card International Association (PCMCIA) slots that allow for software upgrades through the use of Flash memory cards

Note The Cisco uBR7246 VXR chassis does not support the MC11-FPGA cable interface line card.

## Cisco uBR7246 Universal Broadband Router

The Cisco uBR7246 offers an industry-proven CMTS and carrier-class router in a scalable platform to support data, voice, and video services for medium to large network installations. The Cisco uBR7246 provides the following major hardware features:

- Network processing engine
- I/O controller
- Up to two network interface port adapters
- Up to four cable interface line cards
- Up to two removable power supplies providing load-sharing and redundancy capabilities
- Two PCMCIA slots that allow for software upgrades through the use of Flash memory cards

## Cisco uBR7223 Universal Broadband Router

The Cisco uBR7223 is a cost-effective, scalable interface between subscriber CMs and the backbone data network, and is designed specifically for small to medium network installations.

The Cisco uBR7223 provides the following major hardware features:

- Network processing engine
- I/O controller
- One network interface port adapter
- Up to two cable interface line cards
- One removable power supply (The Cisco uBR7223 does not feature load-sharing and redundant power supply capability like the Cisco uBR7246 VXR and Cisco uBR7246.)
- Two PCMCIA slots that allow for software upgrades through the use of Flash memory cards

# Supported Hardware on the Cisco uBR7200 Series

Table 1-5 provides a quick overview of the major hardware features of the Cisco uBR7200 series routers.

*Table 1-5 Cisco uBR7200 Series Hardware Overview*

| Supported Hardware | Cisco uBR7246 VXR | Cisco uBR7246 | Cisco uBR7223 |
|---|---|---|---|
| Network Processing Engines | One of the following:<br>• UBR7200-NPE-G1<br>• NPE-225<br>• NPE-300<br>• NPE-400 | One of the following:<br>• NPE-150<br>• NPE-200<br>• NPE-225 | One of the following:<br>• NPE-150<br>• NPE-200<br>• NPE-225 |
| I/O Controllers | One of the following:<br>• UBR7200-I/O<br>• UBR7200-I/O-FE<br>• UBR7200-I/O-2FE/E | One of the following:<br>• UBR7200-I/O<br>• UBR7200-I/O-FE | One of the following:<br>• UBR7200-I/O<br>• UBR7200-I/O-FE |
| Network Interface Port Adapters | Up to two | Up to two | One |
| Cable Interface Line Cards | Up to four | Up to four | Up to four |
| Removable Power Supplies | Up to two | Up to two | One |
| PCMCIA Slots | Two | Two | Two |

**Note** Earlier release notes stated that the NPE-175 was also supported on the Cisco uBR7200 series routers. Because the NPE-175 has reached its end of life and was never made available for order on the Cisco uBR7200 series routers, it has been removed from the table.

The UBR7200-NPE-G1 does not require that an I/O controller be installed. Refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200rn/index.htm

## Network Processing Engines

The Cisco uBR7246 VXR supports the following Network Processing Engines (NPEs):

- UBR7200-NPE-G1
- NPE-225
- NPE-300
- NPE-400

The Cisco uBR7223 and the Cisco uBR7246 support the following Network Processing Engines (NPE) :

- NPE-150
- NPE-200
- NPE-225

**Note** The NPE-300 and NPE-400 are not supported on the Cisco uBR7223 and the Cisco uBR7246. The NPE-150 and NPE-200 are not supported on the Cisco uBR7246 VXR.

For more information, refer to the following resources on Cisco.com:

- *Network Processing Engine and Network Services Engine Installation and Configuration Guide*
- *Memory Replacement Instructions for the Network Processing Engine or Network Services Engine and Input/Output Controller*

## I/O Controllers

The Cisco uBR7200 series universal broadband routers support the following input/output (I/O) controllers:

- UBR7200-I/O-2FE/E input/output controller
  - Features two Fast Ethernet ports and one Ethernet port.
  - Equipped with 2 RJ-45 receptacles for 10/100 Mbps operation.
  - Supported for the Cisco uBR7246VXR router.
  - The Cisco IOS Release 12.1(10)EC boot helper image [ubr7200-boot-mz.12.1-10.EC] must be used on this controlle.r
- UBR7200-I/O-FE
  - Features one Fast Ethernet port.
  - Equipped with an MII receptacle and an RJ-45 receptacle for use at 100 Mbps full-duplex or half-duplex operation.
  - Only one receptacle can be configured for use at a time.
  - Supported for Cisco uBR7223, Cisco uBR7246, and Cisco uBR7246 VXR routers.
  - The 12.0(15)SC [ubr7200-boot-mz.12.0-15.SC] boot helper image is recommended for this controller.
- UBR7200-I/O
  - Has no Fast Ethernet port.
  - Supported for Cisco uBR7223, Cisco uBR7246, and Cisco uBR7246 VXR routers.
  - The 12.0(15)SC [ubr7200-boot-mz.12.0-15.SC] boot helper image is recommended for this controller.

Note The Single-Port Fast Ethernet I/O Controller (UBR7200-I/O-FE) reached its End of Sale (EOS) point on June 30, 2003. For details, see the Addendum to Product Bulletin, No. 1725, available at the following location on Cisco.com:

http://www.cisco.com/en/US/products/hw/cable/ps2217/prod_eol_notice09186a00800a470d.htm

Note Do not use the 12.1(10)EC boot helper image with the UBR7200-I/O-FE and UBR7200-I/O controllers.

## Network Interface Port Adapters

The Cisco uBR7200 series routers support multiple port adaptors with Ethernet, Gigabit Ethernet and Serial versions. Enhancements and options are available in multiple Cisco IOS Software release trains. For the latest information about supported port adaptors, refer to *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200rn/index.htm

Note Not all Cisco uBR7200 series routers support all port adapters. Some port adapters must be at certain revision levels to be used in the Cisco uBR7246 VXR router.

Note Cisco recommends using the most current release in a release train if possible.

## Cable Interface Line Cards

The Cisco uBR7200 series supports the following cable interface line cards, all of which provide connection to the hybrid fiber-coaxial (HFC) network.

Table 1-6 provides a quick overview of the cable interface line cards that are supported with Cisco uBR7200 series routers.

*Table 1-6 Cisco uBR7200 Series Cable Interface Line Cards*

| Cable Interface Line Card | Upstream Ports | Downstream Ports | Additional Features |
|---|---|---|---|
| MC11C | 1 | 1 | |
| MC12C | 2 | 1 | |
| MC14C | 4 | 1 | |
| MC16C | 6 | 1 | |
| MC16E | 6 | 1 | EuroDOCSIS (Annex A) Support |
| MC16S | 6 | 1 | Enhanced software- and hardware-based Spectrum Management Support |
| MC28C | 8 | 2 | |
| MC28C-BNC | 8 | 2 | BNC connectors instead of F-connectors |

For the latest information about supported cable interface line cards, refer to *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200rn/index.htm

# System Interoperability

This section describes guidelines about the interoperability of certain features in the Cisco uBR7200 series universal broadband routers. Additional DOCSIS interoperability is described in the "Supported Software Features for the Cisco uBR7200 Series" section on page 1-22.

## Cable Modem Interoperability

The Cisco uBR7200 series interoperates with the following cable modems:

- DOCSIS-based two-way cable modems that support basic Internet access, VoIP, or Virtual Private Networks (VPNs).
- Telco-return Cable modems

  To support telco return, use a Cisco uBR7200 series software image that contains "t" in its file name. The telco-return cable modem must be DOCSIS-based or compliant and must be configured to support telco return.

  Note Some third-party telco-return CMs cannot receive traffic over the same downstream channel as CMs operating on a two-way data system. In these instances, segment your cable plant to allow more than one downstream channel.

- EuroDOCSIS cable modems or STBs with integrated EuroDOCSIS CMs using Cisco MC16E cable interface line cards and Cisco IOS Release 12.1(2)EC1 or higher.

  EuroDOCSIS operation support includes 8-MHz Phase Alternating Line (PAL) or Systeme Electronique Couleur Avec Memoire (SECAM) channel plans.

## Clock Synchronization

The Cisco uBR7200 series support clock hardware and software to enable high-quality delivery of IP telephony services through synchronized data transmissions. To support the clock feature set, a Cisco uBR7246 VXR chassis must be used. The Cisco uBR7246 VXR must contain a clock card and an MC16S, MC16E, or MC28C cable interface line card. Only the MC16S, MC16E, and MC28C cable interface line cards support the external clock reference from the clock card to distribute that signal to CMs or STBs attached to the specific network segments. A chassis configured with an MC16S or MC16E cable interface line card must be running Cisco IOS Release 12.1(2)EC1 or higher. A chassis configured with an MC28C cable interface line card must be running Cisco IOS Release 12.1(3a)EC1 or higher.

Each cable modem must also support VoIP applications and the clock reference feature set to enable synchronized timing. The Cisco uBR924 cable access router, running Cisco IOS Release 12.0(7)T or later, supports the clock reference feature set automatically.

# Cisco uBR7200 Series Router Configuration Overview

This section describes Cisco uBR7200 series router features that require software configuration, and summarizes these features of the Cisco uBR7200 series router:


- Port Adapter and Line Card Slot and Logical Interface Numbering, page 1-15
- MAC-Layer Addressing, page 1-17
- Cable Interface Line Cards, page 1-17
- Cable Interface Line Card Slots, page 1-19
- Interfaces and Physical Ports, page 1-20
- Port Adapter Slots, page 1-20


Refer to the "Cisco uBR7200 Series Router Configuration Tools" section on page 1-31 for additional configuration utilities.

## Port Adapter and Line Card Slot and Logical Interface Numbering

For Cisco uBR7200 series components, the slot number is the chassis slot in which a port adapter or a cable interface card is installed. The logical interface number is the physical location of the interface port on a port adapter. Numbers on a Cisco uBR7200 series router begin with 0. Using a Cisco uBR7246 to illustrate, slot/port positioning is as follows:

- Slot 0—I/O controller
- Slot 1-2—Cisco port adapters
- Slot 3-6—Cisco cable interface line cards; the upstream ports on the card start with port 0.

To configure the system, define the Cisco uBR7200 series interfaces, using the **interface type slot/port** commands:

- Type—Cable
- Slot—Slot number in chassis. Slot numbers begin with 0.
- Port—Port number on a cable interface line card slot. Port numbers begin with a 0.

Configuring Cisco cable interface line cards is particularly important because these components serve as the cable TV RF interfaces. Configuration involves the following tasks for each interface:

- Setting the downstream center frequency for the card to reflect the digital carrier frequency of the downstream RF carrier (the channel) for that downstream port. To do this, enter the fixed center frequency for your downstream RF carrier in Hz:

```
Router (config-int)# cable downstream frequency down-freq-hz
```

Note This command has no effect on the external upconverter, which actually sets the downstream frequency. Noting the correct value for the cable interface line card, however, provides useful information for troubleshooting.

The digital carrier frequency is specified to be the center of a 6 or 8 MHz channel based on your channel plan. To illustrate for NTSC channel plans, EIA channel 95 spans 90.00 to 96.00 MHz. The center frequency is 93.000 MHz which is the digital carrier frequency that should be configured as the downstream frequency.

Tip The digital carrier frequency is not the same as the video carrier frequency. For EIA channel 95, the video carrier frequency is 91.250 MHz which is 1.75 MHz below the center frequency.

- Activating the downstream port on the cable interface line card for data transmission over the HFC network, using the following command:

  ```
  Router (config-int)# no shutdown
  ```

  The particular downstream port LED should light.

- Setting the upstream frequency of your RF output to comply with the expected input frequency of your Cisco cable interface line card.

Tip The valid range for a fixed upstream frequency is 5,000,000 Hz to 65,000,000 Hz for the MC16E cable interface line card. The valid range for all other cable interface line cards that support NTSC operations is 5,000,000 Hz to 42,000,000 Hz.

The cable interface will not operate until you either set a fixed upstream frequency or create and configure a spectrum group. Enter the fixed center frequency for your upstream RF carrier in Hz and specify a port number from 0 to 5:

```
Router (config-int)# cable upstream port frequency up-freq-hz
```

Note Make sure that the selected upstream frequency does not interfere with the frequencies used for any other upstream applications in your cable plant.

- Entering an upstream RF carrier frequency for each upstream port on a cable modem.
- Activating the RF carrier on each upstream port to support data from CMs or set top boxes on your network to the Cisco uBR7200 series router. Enable upstream data traffic, using the following command:

  ```
  Router (config-int)# no cable upstream port shutdown
  ```

  The specified upstream port LED lights.

  Repeat the above for each upstream port to activate.

- Verifying your settings using the following command:

  ```
  Router# show running-config
  ```

- Saving the configuration to nonvolatile random access memory (NVRAM) so that your settings are retained after a power cycle:

  ```
  Router# copy running start
  ```

- Verifying the upstream frequency, using the **show controllers cable** *slot/port* **upstream** command for the upstream port you just configured.
- Verifying the downstream center frequency, using the **show controllers cable** *slot/port* **downstream** command for the downstream port you just configured.

# MAC-Layer Addressing

The Media Access Control (MAC)-layer or hardware address is a standardized data link layer address required for certain network interface types. These addresses are not used by other devices in the network; they are specific and unique to each port. The Cisco uBR7200 series uses a specific method to assign and control the MAC-layer addresses for port adapters.

All LAN interfaces (ports) require unique MAC-layer addresses, also known as hardware addresses. Typically, the MAC address of an interface is stored on a memory component that resides directly on the interface circuitry; however, the online insertion and removal (OIR) feature requires a different method. The OIR feature lets you remove a port adapter or cable interface card and replace it with another identically configured one. If the new port adapter or cable interface card matches the port adapter or cable interface card you removed, the system immediately brings it online.

To support OIR, an address allocator with a unique MAC address is stored in an EEPROM on the universal broadband router midplane. Each address is reserved for a specific port and slot in the router regardless of whether a port adapter or a cable interface card resides in that slot.

Note Port adapter and cable interface card slots maintain the same slot number regardless of whether other port adapters or cable interface cards are installed or removed. However, when you move a port adapter or cable interface card to a different slot, the logical interface number changes to reflect the new slot number.

Caution When “hot swapping” a port adapter or cable interface line card with a different type of component (for example, an MC11 FPGA with an MC11C, or an MC16B with an MC16C), you might have to reconfigure the interfaces. Refer to the *Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide* or appropriate FRU document for more specific information regarding online insertion and removal (OIR).

The MAC addresses are assigned to the slots in sequence. The first addresses are assigned to port adapter slot 0 and slot 1, and the next addresses are assigned to port adapter slot 2 through cable interface card slot 6. This address scheme allows you to remove port adapters or cable interface cards and insert them into other universal broadband routers without causing the MAC addresses to move around the network or be assigned to multiple devices.

Storing the MAC addresses for every slot in one central location means the addresses stay with the memory device on which they are stored.

# Cable Interface Line Cards

As of the date of this publication, the following Cisco cable interface cards can be installed in a Cisco uBR7200 series router:

- MC11 with one downstream modulator and one upstream demodulator. Two different revisions exist for this card:
  - The FPGA version of the card supports the following defaults: Quadrature Amplitude Modulation (QAM)-64 at 27 Mbps downstream, and Quadrature Phase Shift Keying (QPSK) at 1.280 kbps upstream. The card outputs +32 dBmV and +/- 2 dBmV.
  - The C version of the card supports the following defaults: QAM-256 at 40 Mbps downstream and QAM-16 at 5 Mbps upstream. The card supports upstream channel widths of 200 kHz, 400 kHz, 800 kHz, 1.6 MHz, and 3.2 MHz. The card outputs +42 dBmV and +/- 2 dBmV.

Note All C version cards support all DOCSIS modulation and symbol rates. Refer to Table 1-7Table 1-6 for a list of DOCSIS supported data rates and modulation schemes.

Because the FPGA version of the MC11 card supports only one upstream modulation and channel width, you cannot define an upstream modulation profile for the card. The default modulation profile 1 cannot be changed when using the FPGA version of the MC11 card.

- MC12C with one downstream modulator and two upstream demodulators: The card supports the following defaults: QAM-256 at 40 Mbps downstream and QAM-16 at 5 Mbps upstream. The card supports upstream channel widths of 200 kHz, 400 kHz, 800 kHz, 1.6 MHz, and 3.2 MHz.The card outputs +42 dBmV and +/- 2 dBmV.
- MC14C with one downstream modulator and four upstream demodulators: The card supports the following defaults: QAM-256 at 40 Mbps downstream and QAM-16 at 5 Mbps upstream. The card supports upstream channel widths of 200 kHz, 400 kHz, 800 kHz, 1.6 MHz, and 3.2 MHz. The card outputs +42 dBmV and +/- 2 dBmV.
- MC16 with one downstream modulator and six upstream demodulators. Two different revisions exist for this card:
  - The B version of the card supports the following defaults: QAM-64 at 27 Mbps downstream and QPSK at 2.56 Mbps upstream. The card supports channel widths of 200 kHz, 400 kHz, 800 kHz, 1.6 MHz, and 3.2 MHz. The card outputs +32 dBmV and +/- 2 dBmV.

    Note The B version card excludes support of QAM-256 downstream and QAM-16 upstream support at two of the five DOCSIS upstream symbol rates—2.56 M and 1.28 M. Refer to Table 1-7Table 1-6 for Table 1-6a list of DOCSIS supported data rates and modulation schemes.

  - The C version of the card supports the following defaults: QAM-256 at 40 Mbps downstream and QAM-16 at 5 Mbps upstream. The card supports upstream channel widths of 200 kHz, 400 kHz, 800 kHz, 1.6 MHz, and 3.2 MHz. The card outputs +42 dBmV and +/- 2 dBmV.
- MC16S with one downstream modulator and six upstream demodulators. The card supports the following defaults: QAM-256 at 40 Mbps downstream and QAM-16 at 5 Mbps upstream. The card supports upstream channel widths of 200 kHz, 400 kHz, 800 kHz, 1.6 MHz, and 3.2 MHz. The card outputs +42 dBmV and +/- 2 dBmV.

  The MC16S includes the ability to scan portions of the upstream spectrum for clean channels of varying widths. A daughtercard on the MC16S samples the 5-to-42 MHz upstream spectrum and initiates a frequency hop if an administrator-defined threshold value for offline CMs is met. The threshold value is contained in the router's configuration file. When the threshold value is reached, the spectrum management daughtercard takes a snapshot of the available upstream spectrum and passes this information to the Cisco IOS software where it is analyzed for indications of significant ingress or impulse noise. From this analysis, the Cisco IOS software draws informed conclusions on the cleanest portion(s) of the upstream frequency spectrum to switch to and initiates a frequency hop.
- MC16E with one downstream modulator and six upstream demodulators. The card supports the following defaults: QAM-256 at 40 Mbps downstream and QAM-16 at 5 Mbps upstream. The card supports EuroDOCSIS 8 MHz PAL and SECAM channel plans, supporting downstream rates of 85-to-860 MHz range with upstream ranges of 5-to-65 MHz. The card outputs +40 dBmV and +/- 2 dB.

Note While most Cisco cable interface line cards transmit downstream signals to upconverters using a 44 MHz frequency, the MC16E transmits downstream IF signals to an upconverter using the 36.125 MHz frequency. Only the MC16E cable interface line card supports full 8 MHz operation.

The cable interface cards can be configured in a number of different upstream combinations based on the card used, your cable network, and the anticipated subscription and service levels. Table 1-7 shows the DOCSIS and EuroDOCSIS data rates.

*Table 1-7 DOCSIS and EuroDOCSIS Data Rates*

| Upstream Channel Width | Modulation Scheme | Baud Rate Sym/sec | Raw Bit Rate Mbit/sec |
|---|---|---|---|
| 3.2 MHz | QAM-16<br>QPSK | 2.56 M | 10.24<br>5.12 |
| 1.6 MHz | QAM-16<br>QPSK | 1.28 M | 5.12<br>2.56 |
| 800 kHz | QAM-16<br>QPSK | 640 K | 2.56<br>1.28 |
| 400 kHz | QAM-16<br>QPSK | 320 K | 1.28<br>0.64 |
| 200 kHz | QAM-16<br>QPSK | 160 K | 0.64<br>0.32 |

# Cable Interface Line Card Slots

To display information about a specific cable interface card slot's downstream channel, use the **show interfaces cable** command with the cable modem line card's slot number and downstream port number in the following format:

**show interfaces cable** *slot/downstream-port* [**downstream**]

Use the slot number and downstream port number to display information about a downstream interface. You can abbreviate the command to **sh int c**. The following example illustrates the display for downstream channel port 0 in cable interface slot 3 of a Cisco uBR7246:

```
Router# sh int c 3/0

Cable3/0 is up, line protocol is up
    Hardware is CMTS, address is 0009.0ed6.ee18 (bia 0009.0ed6.ee18
    Internet address is 1.1.1.1/24
    MTU 1500 bytes, BW 27000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
    Encapsulation MCNS, loopback not set, keepalive not set
    ARP type: ARPA, ARP Timeout 04:00:00
    Last input 00:00:00, output 00:00:00, output hang never
    Last clearing of "show interface" counters never
    Queueing strategy: fifo
    Output queue 0/40, 0 drops; input queue 0/75, 0 drops
    5 minute input rate 41000 bits/sec, 45 packets/sec
    5 minute output rate 43000 bits/sec, 45 packets/sec
        1616534 packets input, 184284660 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1616534 packets output, 184284660 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 output buffer failures, 0 output buffers swapped out
```

To display information about a specific cable interface card slot's upstream channel, use the **show interfaces cable** command with the cable modem card's slot number, downstream port number, and upstream port number in the format of **show interfaces cable** *slot/downstream-port* [**upstream**] *upstream-port*. Use the slot number, downstream port number, and upstream port number to display information about an upstream interface. You can abbreviate the command to **sh int c**.

The following example shows the display for upstream channel port 0 in cable interface slot 3 of a Cisco uBR7246 that is turned up:

```
Router# sh int c 3/0 0

Cable6/0: Upstream 0 is up
    Received 3699 broadcasts, 0 multicasts, 28586 unicasts
    0 discards, 0 errors, 0 unknown protocol
    21817 packets error-free, 2371 corrected, 8097 uncorrectable
    0 noise, 0 microreflections
    CBR_queue_depth: [not implemented], ABR_queue_depth: [not implemented],
    UBR[1]_queue_depth: 0, UBR[2]_queue_depth: 0,
    UBR[3]_queue_depth: 0,  POLLS_queue_depth:  [not implemented]
    ADMIN_queue_depth: [not implemented]
    Last Minislot Stamp (current_time_base):190026    FLAG:1
    Last Minislot Stamp (scheduler_time_base):200706  FLAG:1
```

# Interfaces and Physical Ports

Table 1-8 maps the cable interface card's interfaces and physical ports. The cards can be configured in a number of different upstream combinations.

*Table 1-8 Interface to Port Mapping*

| Cable Interface Line Card | Interface | Physical Ports |
|---|---|---|
| MC11 | Cable N/0 | DS, US0 |
| MC12 | Cable N/0 | DS, US0, US1 |
| MC14 | Cable N/0 | DS, US0, US1, US2, US3 |
| MC16 | Cable N/0 | DS, US0, US1, US2, US3, US4, US5 |

# Port Adapter Slots

You can display information on a specific port adapter or all port adapters in the Cisco uBR7200 series. To display information about all port adapter slots, use the **show interfaces** command. To display information about a specific port adapter slot, use the **show interfaces** command with the port adapter type and slot number in the format of **show interfaces** [*type slot/port*].

Tip If you abbreviate the command (**sh int**) and do not specify the port adapter type and slot number (or arguments), the system interprets the command as **show interfaces.** The system displays the status of all port adapters, all cable interface cards, and all ports.

The follow example illustrates the **show interfaces** command with status information (including the physical port adapter number) for each port adapter and cable interface card in the Cisco uBR7246 router:

```
Router# sh int

FastEthernet0/0 is administratively up, line protocol is up
Hardware is DEC21140, address is 0000.0000.0000 (bia 0000.0000.0000)
Internet address is 1.1.1.3
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
(display text omitted)
Hssi1/0 is administratively down, line protocol is down
Hardware is MIF68840_MM, address is 0000.0000.0000 (bia 0000.0000.0000)
Internet address is 1.1.1.0
MTU 4470 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
(display text omitted)
Ethernet2/0 is administratively up, line protocol is up
Hardware is AmdP2, address is 0000.0000.0000 (bia 0000.0000.0000)
Internet address is 1.1.1.7
MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
(display text omitted)
Cable3/0 is up, line protocol is up
Hardware is CMTS, address is 0009.0ed6.ee18 (bia 0009.0ed6.ee18)
Internet address is 1.1.1.1/24
MTU 1500 bytes, BW 27000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
(display text omitted)
```

You can also use arguments such as the interface type (Ethernet, Fast Ethernet, ATM, serial, HSSI, Packet-over-SONET, and so forth) and the port address (slot/port) to display information about a specific port adapter interface only. The following example shows such a display:

```
Router# sh int f1/0
FastEthernet1/0 is up, line protocol is up
  Hardware is AmdFE, address is 0030.7bfa.a81c (bia 0030.7bfa.a81c)
  Internet address is 111.0.1.18/30
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy:fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets put, 230925 bytes
     Received 146107 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     0 packets put, 284529 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

# Supported Software Features for the Cisco uBR7200 Series

This section summarizes Cisco uBR7200 series router software features for all supported Cisco IOS Release trains, and directs you to additional configuration information for each feature.

## Cisco uBR7200 Series Router Features and Cisco IOS Releases

Table 1-9 summarizes the software-related features and related Cisco IOS releases that support the Cisco uBR7200 series router. Cisco IOS features indicate the first release in which the feature was introduced. Unless otherwise noted, feature support continues in later releases of the same or related Cisco IOS release train

Many additional features were introduced in release trains prior to those listed above, such as 12.0 T, 12.0 SC, 12.1 XF and other earlier releases that may no longer be supported on the Cisco uBR7200 Series. Refer to the release notes for your respective Cisco IOS release for additional feature support and image information.

*Table 1-9 Cisco uBR7200 Series Routers Features by Cisco IOS Release*

| Feature | Supporting Cisco IOS Releases |
|---|---|
| Cisco uBR7200 Series Router Configuration Tools | |
| Autoinstall | 12.0 T, 12.0 XR, 12.0 SC, 12.1 EC, 12.1 CX, 12.2 BC and 12.3 BC releases |
| Cable Interface Setup Facility | 12.1 EC, 12.1 CX, 12.2 BC and 12.3 BC releases |
| Cable Interface Extended Setup Facility | 12.1(3a)EC1 and all later Cisco IOS releases supporting the Cisco uBR7200 Series CMTS |
| Cisco Network Registrar | 12.1 EC, 12.2 BC, 12.3 BC |
| Interface Range Specification | 12.0 T, 12.0 XR, 12.0 SC, 12.1 EC, 12.1 CX, 12.2 BC and 12.3 BC releases |
| Internal Modem Configuration File Editor | 12.2(1)XF1 and later 12.2 XF, 12.2 BC and 12.3 BC releases |
| Manual Configuration Mode for the Cisco uBR7200 Series CMTS | All Cisco IOS releases supporting the Cisco uBR7200 Series CMTS |
| Virtual Interface Support and Frequency Stacking Support | 12.3(9a)BC and later 12.3 BC releases |
| Bandwidth Management Features | |
| Load Balancing Support | 12.3(9a)BC and later 12.3 BC releases |
| Cisco IOS Command-Line Enhancements | |
| exec prompt timestamp Command | 12.1(12c)EC, 12.2(8)BC2 and later 12.1 EC, 12.2 BC and 12.3 BC releases |
| show Command Enhancements | Multiple Cisco IOS software releases. Enhancements include:<br>• show cable qos<br>• show int cx/y sid<br>• show cable modem<br>• show cable modulation-profile<br>• show cable modem summary |

*Table 1-9 Cisco uBR7200 Series Routers Features by Cisco IOS Release (continued)*

| Feature | Supporting Cisco IOS Releases |
|---|---|
| Cisco IOS Release 12.3(9a)BC Command-Line Interface (CLI) Enhancements | 12.3(9a) enhancements to or introductions of the following commands:<br>• cable logging layer2events<br>• cable source-verify<br>• show cable tech-support<br>• show controllers cable<br>• show tech-support |
| Cisco Quality of Service Features | |
| Cisco Network-Based Application Recognition (NBAR) | 12.1(10)EC, 12.2 BC and later releases |
| RTP Header Compression | 11.3(11)NA, 12.0 T and later releases |
| DHCP Servers and Feature Support | |
| Configurable Leasequery Server | 12.3(17a)BC and later 12.3 BC releases |
| DHCP MAC Address Exclusion List for cable-source verify dhcp Command | 12.3(13a)BC and later 12.3 BC releases<br>See the "DOCSIS 1.1 Feature Support" section on page 1-57 for additional DHCP features. |
| DOCSIS 1.0 Feature Support | |
| DOCSIS 1.0 Baseline Privacy | 12.0(6)SC, 12.1 EC and later releases |
| DOCSIS 1.0 Baseline Privacy Interface Encryption and Encrypted Key Exchange | 12.0 SC and later releases in multiple release trains |
| DOCSIS 1.0 Concatenation Override Featurette | 12.3(13a)BC and later 12.3 BC releases |
| DOCSIS 1.0 Extensions | 12.0(16)SC3, 12.1 EC, 12.2 CX, 12.2 BC, and 12.3 BC |
| DOCSIS 1.0 Quality of Service | 12.1 EC, 12.2 CX, 12.2 BC, and 12.3 BC<br>Several additional DOCSIS 1.0 QoS enhancements for the Cisco uBR7200 Series are described in release notes for earlier releases. |
| DOCSIS Quality of Service Enhancements Prior to DOCSIS 1.1 | DOCSIS quality of service (QoS) enhancements added to Cisco IOS Release 12.1(1a)T1 and continue with later releases in multiple trains. |
| DOCSIS 1.0 ToS Overwrite | 12.3(17a)BC2 and later 12.3 BC releases. |
| DOCSIS Customer Premises Equipment Configurator | DOCSIS CPE Configurator V2.0.4 and V 3.2 supported in multiple Cisco IOS releases. |
| Enhanced Rate Bandwidth Allocation (ERBA) Support for DOCSIS 1.0 Cable Modems | 12.3(13a)BC and later 12.3 BC releases |

*Table 1-9 Cisco uBR7200 Series Routers Features by Cisco IOS Release (continued)*

| Feature | Supporting Cisco IOS Releases |
|---|---|
| DOCSIS 1.0+ Feature Support | |
| Concatenation for DOCSIS 1.0+ | 12.1(1)T and later releases in multiple trains support DOCSIS 1.0+ on the Cisco uBR7200 Series. |
| Dynamic MAC messages | |
| Multiple SIDs per Cable Modem | |
| Separate Downstream Rates | |
| Unsolicited Grant Service (CBR-scheduling) on the Upstream | |
| DOCSIS 1.1 Feature Support | |
| Baseline Privacy Interface Plus (BPI+) | 12.2(4)BC1 and later 12.2 BC and 12.3 BC releases |
| Burst Profile Configuration | 12.2(4)BC1 and later 12.2 BC and 12.3 BC releases |
| Cable Modulation Profile Default Templates | 12.1(3a)EC1 and later 12.1 EC releases |
| DHCP Cable Modem Host ID | 12.0(4)T, with additional enhancements and support in 12.0 (6) SC, 12.1(2) EC1, 12.1(3a)EC, 12.2(15)BC2 and later releases |
| DHCP Client ID/Remote ID Options | 12.0(16)SC3 and later releases in multiple release trains |
| DHCP, Time of Day (ToD) and TFTP Servers | Multiple releases in multiple release trains beginning with 12.0 early deployment releases |
| DOCSIS 1.1 Quality of Service Features | 12.2 BC and 12.3 BC release trains, with additional DOCSIS 1.1 features supported in certain earlier Cisco IOS 12.1 EC and 12.0 SC release trains. Includes:<br>• Concatenation for DOCSIS 1.1<br>• DOCSIS 1.0 and 1.0+ Cable Modem Support<br>• DOCSIS 1.1 Service Flow Model<br>• Downstream QoS Handling Supported<br>• Dynamic MAC Messages<br>• Dynamic Map-Advance<br>• Dynamic SID Support<br>• Fragmentation (Layer 2)<br>• Multiple SID Support<br>• Payload Header Suppression (PHS)<br>• QoS Configuration<br>• QoS Profile Enforcement<br>• Time-of-Day Server<br>• Trivial File Transfer Protocol Server<br>• Type/Length/Value Parser and Encoder<br>• Upstream Address Verification<br>• Upstream QoS Improvements<br>• Upstream QoS Models Supported |

*Table 1-9 Cisco uBR7200 Series Routers Features by Cisco IOS Release (continued)*

| Feature | Supporting Cisco IOS Releases |
|---|---|
| DOCSIS 1.1 Two-way Transmission (Cisco uBR7246VXR Router) | 12.2 BC, 12.3 BC |
| Downstream Channel ID | 12.0(4)T and later releases in multiple trains |
| Downstream Frequency Override | 12.0(6)SC, 12.1 EC and later releases supporting the Cisco uBR7200 series |
| Downstream Packet Classifier | 12.2 BC and 12.3 BC release trains |
| Downstream Packet Scheduler | 12.2 BC and 12.3 BC release trains |
| Downstream Rate Shaping with IP Type of Service Bits | 11.3NA, 12.0(5)T and later releases in multiple release trains. |
| Downstream Traffic Shaping | 11.3(6) NA, with additional enhancements and support in 12.0(4)XI, 12.0(5)T1, 12.1(1)EC1, 12.2(4)BC1 and later releases. |
| Optional Upstream Scheduler Modes | 12.3(13a)BC and later 12.3 BC releases |
| DOCSIS 2.0 Feature Support | |
| DOCSIS 2.0 A-TDMA Support | 12.2(15)CX and continues with later 12.2 CX, 12.2 BC and 12.3 BC releases |
| High Availability Features | |
| Cisco DDC (Dual DOCSIS Channel) | 12.3(9a)BC and later 12.3 BC releases |
| DSX Messages and Synchronized PHS Information | 12.3(17a)BC and later 12.3 BC releases |
| HCCP Support for the Cisco uBR-MC16S Cable Interface Line Card | 12.1(7)EC and later releases in multiple release trains |
| HCCP N+1 Redundancy | 12.1(10)EC, with additional enhancements and support in 12.2(4)XF1, 12.2(4)BC1, 12.2(8)BC2, 12.2(11)BC1, 12.2(15)BC1, 12.2(15)BC2a and later releases in multiple trains |
| High Availability Features in Cisco IOS Release 12.3(13a)BC | 12.3(13a)BC and later 12.3 BC releases |
| Hot-Standby 1+1 Redundancy | 12.1(3a)EC and later releases in multiple release trains |
| IF Muting for HCCP N+1 Redundancy | 12.2(15)BC2a and later 12.2 BC and 12.3 BC releases |
| Intercept Features | |
| Access Control List Support for COPS Intercept | 12.3(13a)BC and later 12.3 BC releases |
| Cable Monitor Enhancements | 12.3(17a)BC and later 12.3 BC releases |
| COPS TCP Support for the Cisco Cable Modem Termination System | 12.3(13a)BC and later 12.3 BC releases |
| Service Independent Intercept (SII) Support on the Cisco uBR7200 Series | 12.3(13a)BC and later 12.3 BC releases |

*Table 1-9 Cisco uBR7200 Series Routers Features by Cisco IOS Release (continued)*

| Feature | Supporting Cisco IOS Releases |
|---|---|
| IP Broadcast and Multicast Features | |
| Multicast QoS Support on the Cisco uBR7246VXR CMTS | 12.3(13a)BC and later 12.3 BC releases |
| IP Routing Features | |
| Cable ARP Filter Enhancement | 12.2(15)BC2b and later 12.2 BC and 12.3 BC releases |
| Cable Interface Bundling and Cable Subinterfaces | 12.0 SC, 12.1 EC, 12.2 BC and later BC releases |
| Configurable Alternate Termination System Information Messages | 12.1(2)EC and later releases in this and additional release trains |
| Easy IP (Phase 1) | 12.0 XC and later releases in this and additional release trains |
| Fast-Switched Policy Routing | 12.0 XC and later releases in this and additional release trains |
| HSRP over ISL in Virtual LAN Configurations | 12.0 XC and later releases in this and additional release trains |
| IP Enhanced IGRP Route Authentication | 12.0 XC and later releases in this and additional release trains |
| IP Network Address Translation/Port Address Translation | 12.0 XC and later releases in this and additional release trains |
| NAT—Support for NetMeeting Directory (Internet Locator Service—ILS) | 12.0 XC and later releases in this and additional release trains |
| Router-Port Group Management Protocol | 12.1 T and later releases in this and additional release trains |
| Supported Protocols on the Cisco uBR7200 Series | Multiple protocols are supported in all release trains that support the Cisco uBR7200 Series. |
| Management Features | |
| Admission Control for the Cisco CMTS | 12.3(13a)BC and later 12.3 BC releases |
| Cable ARP and Proxy ARP (cable arp and cable proxy arp commands) | 12.1T , 12.0(6)SC , 12.1(2) EC1, 12.2(8)BC1, and later releases in respective release trains |
| cable map-advance Command Enhancements | 12.1 EC and later releases in multiple release trains |
| cable monitor Command | 12.0(6)EC with additional enhancements and support in later releases in multiple release trains |
| cable intercept Command | 12.0(5)T1, 12.0(6)SC, 12.1(2)EC, 12.2(4)BC1 and later releases in respective release trains |
| DOCSIS 2.0 SAMIS ECR Data Set | 12.3(17a)BC and later 12.3 BC releases |
| Downstream Load Balancing Distribution with Upstream Load Balancing | 12.3(17b)BC and later 12.3 BC releases |
| Dynamic Channel Change (DCC) for Loadbalancing | 12.3(17a)BC and later 12.3 BC releases |

*Table 1-9 Cisco uBR7200 Series Routers Features by Cisco IOS Release (continued)*

| Feature | Supporting Cisco IOS Releases |
|---|---|
| Dynamic Ranging Support | 12.1 EC and later releases in this and multiple release trains |
| Load Balancing for the Cisco CMTS | 12.2(15)BC1 and later releases in the 12.2 BC and 12.3 BC release trains |
| Management Information Base (MIB) Changes and Enhancements | 12.3(17a)BC and later 12.3 BC releases |
| MAX-CPE Override for Cable Modems | 12.1(2)EC1 and later releases or release trains |
| Per-Modem Error Counter Enhancements | 12.1(4)CX, 12.2(1)XF, and 12.2(4)BC1 and later releases in these release trains |
| Pre-equalization Control for Cable Modems | 12.3(17a)BC and later 12.3 BC releases |
| Subscriber Traffic Management (STM) Version 1.1 | 12.3(9a)BC and later 12.3 BC releases |
| Usage Based Billing (SAMIS) | 12.3(9a)BC and later 12.3 BC releases |
| Multicast Features | |
| Bidirectional PIM | 12.1 EC, 12.2 BC |
| DOCSIS Set-top Gateway (DSG) 1.0 | 12.3(9a)BC and later 12.3 BC releases |
| Advanced-mode DOCSIS Set-Top Gateway Issue 1.1 | 12.3(13a)BC and later 12.3 BC releases |
| Advanced-mode DOCSIS Set-Top Gateway Issue 1.2 | 12.3(17a)BC2 and later 12.3 BC releases |
| IGMP Version 3 | 12.1(3)T and later releases in multiple release trains |
| IP Multicast Load Splitting across Equal-Cost Paths | 12.0 XC and later releases in this and additional release trains |
| IP Multicast over ATM Point-to-Multipoint Virtual Circuits | 12.0 XC and later releases in this and additional release trains |
| IP Multicast over Token Ring LANs | 12.0 XC and later releases in this and additional release trains |
| Source Specific Multicast | 12.0 XC and later releases in this and additional release trains |
| Stub IP Multicast Routing | 12.0 XC and later releases in this and additional release trains |
| PacketCable and Voice Support Features | |
| PacketCable 1.0 With CALEA | 12.3(13a)BC and later 12.3 BC releases |
| Security Features | |
| Access Control Lists | 12.2(4)XF1 and later XF and BC releases<br>12.2(10)EC and later EC releases |
| Automated Double Authentication | 12.0 XC and later releases in this and additional release trains |
| Cable Modem and Multicast Authentication Using RADIUS | 12.0 XC and later releases in this and additional release trains |
| Cable Source Verification (cable source-verify Command) | 11.3 XA with additional support and enhancements in later releases in additional release trains |

*Table 1-9 Cisco uBR7200 Series Routers Features by Cisco IOS Release (continued)*

| Feature | Supporting Cisco IOS Releases |
|---|---|
| Cisco IOS Firewall Feature Set | 12.0(1)T and later releases in this and additional release trains |
| Cisco IOS Firewall Feature Enhancements | 12.1 XM and later releases in this and additional release trains |
| Dynamic Mobile Hosts | 12.1 CX, 12.2(4)XF and later releases in this and additional release trains |
| Dynamic Shared Secret for DOCSIS | 12.2(15)BC1 and later releases in the 12.2 BC and 12.3 BC release trains |
| Dynamic Shared Secret (DMIC) with OUI Exclusion for DOCSIS | 12.3(9a)BC and later 12.3 BC releases |
| HTTP Security | 12.2(4)BC1 and later releases in this and additional release trains |
| Named Method Lists for AAA Authorization & Accounting | 12.0 T, 12.0 CX, and later releases in these and additional release trains |
| Per-Modem Filters (Per-Modem and Per-Host Access Lists) | 12.0(5)T1, 12.0(6)SC, and later releases in these and additional release trains |
| Per-User Configuration | 12.0 T and later releases in this and additional release trains |
| Redirect-Number Support for RADIUS and TACACS+ Servers | 12.0(4)XI with additional support and enhancements in later releases in additional release trains |
| Reflexive Access Lists | 12.0 XC and later releases in this and additional release trains |
| Secure Shell (SSH) Supported in "k1" Images for Cisco uBR7200 | 12.1(1)T, 12.2(2)XA, 12.2 CX and later releases in this and additional release trains |
| Turbo Access Control Lists | 12.1 EC, 12.2 CX, 12.2(4)XF1 and later releases in these and additional release trains |
| Vendor-Proprietary RADIUS Attributes | 11.3(11)NA, 12.0 T and later releases in these and additional release trains |
| SNMP Features and Enhancements | |
| Individual SNMP Trap Support | 12.1(3)T and later releases in this and additional release trains |
| LinkUp/Down Traps Support (RFC 2233) | 12.1 EC and later releases in this and additional release trains |
| SNMPv2C | 12.0 XC and later releases in this and additional release trains |
| SNMPv3 | 12.0 T and later releases in this and additional release trains |
| SNMP Cable Modem Remote Query | 12.1 EC and later releases in this and additional release trains |
| SNMP Management Information Base (MIB) Enhancements | Multiple Cisco IOS releases and release trains |
| SNMP MIBs Changes and Updates in Cisco IOS Release 12.3(9a)BC | 12.3(9a)BC and later 12.3 BC releases |
| SNMP Warm Start Trap | 12.1 CX, 12.1 EC and later releases in these and additional release trains |
| Spectrum Management and Advanced Spectrum Management Features | |
| Advanced Spectrum Management | 12.1 CX and later releases in this and additional release trains |

*Table 1-9 Cisco uBR7200 Series Routers Features by Cisco IOS Release (continued)*

| Feature | Supporting Cisco IOS Releases |
|---|---|
| Cable Modulation Profile Default Templates | 12.1 EC and later releases in this and additional release trains |
| Downstream Traffic Shaping | 12.0(7)XR2, 12.2(2)XF1 and later releases in these and additional release trains |
| Dynamic Upstream Modulation | 12.1(3)EC and later releases in this and additional release trains |
| Guided and Scheduled Spectrum Management | Refer to the following features:<br>• Traffic Shaping (Downstream or Upstream)<br>• Frequency Hopping Capabilities<br>• Dynamic Upstream Modulation (SNR-based)<br>• Input Power Levels |
| Input Power Levels | 11.3 NA, with additional enhancements in 12.0(7)XR2, 12.0(13)SC, 12.1(4)EC, 12.2(4)BC1 and later releases in these release trains |
| Spectrum Management Enhancements in Cisco IOS Release 12.3(9a)BC | 12.3(9a)BC and later 12.3 BC releases |
| Upstream Traffic Shaping | 11.3(9)NA and later releases in this and additional release trains |
| Testing, Troubleshooting and Diagnostic Features | |
| Cable Downstream Frequency Override | 12.0 SC, 12.1 EC, 12.1T and 12.2BC release trains |
| Cable Flap List | 11.3 NA, 12.0(4)XA, 12.0(7)XR, 12.1(2)EC, 12.1(5)EC, 12.1(7)CX, 12.2(4)BC1 and later releases in these and additional release trains |
| Cisco Broadband Troubleshooter (CBT) 3.2 | 12.3(9a)BC and later 12.3 BC releases |
| Cisco CMTS Static CPE Override | 12.3(9a)BC and later 12.3 BC releases |
| Fast Fault Detection | 12.2(15)BC1 and later 12.2 BC and 12.3 BC releases |
| Virtual Interfaces | |
| Virtual Interface Bundling on the Cisco uBR-MC28/U BPE | |
| VPN and Layer 2 Tunneling Features | |
| Dynamic SID/VRF Mapping Support | 12.3(13a)BC and later 12.3 BC releases |
| NAT—Support for NetMeeting Directory (Internet Locator Service—ILS) | 12.0 XC and later releases in this and additional release trains |
| IPv6 over L2VPN | 12.3(17a)BC and later 12.3 BC releases |
| Mapping Service Flows to MPLS-VPN | 12.2(11)BC2 and later 12.2 BC and 12.3 BC releases |
| MPLS VPN Support for Subinterfaces and Cable Interface Bundles | 12.1 CX, 12.1 EC and later releases in these and additional release trains |

*Table 1-9 Cisco uBR7200 Series Routers Features by Cisco IOS Release (continued)*

| Feature | Supporting Cisco IOS Releases |
|---|---|
| Overlapping Subinterface IP Addresses | 12.1(3)EC and later releases in this and additional release trains |
| Transparent LAN Services (TLS) and L2 Tunneling ATM/SIDs | 12.3(9a)BC and later 12.3 BC releases |
| Transparent LAN Services (TLS) and L2 Virtual Private Networks | 12.3(13a)BC and later 12.3 BC releases |
| VLAN Features | |
| HSRP over ISL in Virtual LAN Configurations | 12.0 XC and later releases in this and additional release trains |
| WAN Optimization and Services Features | |
| Bandwidth Allocation Control Protocol (BACP) | 12.0 XC and later releases in this and additional release trains |
| Closed User Group Selection Facility Suppress Option | 12.1 T, 12.1 XM and later releases in these and additional release trains |
| Enhanced Local Management Interface (ELMI) | 11.3(11)T, 12.0 XC and later releases in these and additional release trains |
| Frame Relay Enhancements | 12.2(4)BC1 and later 12.2 BC and 12.3 BC releases |
| Frame Relay MIB Extensions | 12.0 XC and later releases in this and additional release trains |
| Frame Relay Router ForeSight | 12.0 XC and later releases in this and additional release trains |
| ISDN Advice of Charge | 12.0 XC and later releases in this and additional release trains |
| ISDN Caller ID Callback | 12.0 XC and later releases in this and additional release trains |
| ISDN Multiple Switch Types | 12.0 XC and later releases in this and additional release trains |
| ISDN NFAS | 12.0 XC and later releases in this and additional release trains |
| Microsoft Point-to-Point Compression (MPPC) | 12.0 XC and later releases in this and additional release trains |
| MLPPP Support | 12.3(13a)BC and later 12.3 BC releases |
| National ISDN Switch Types for BRI and PRI | 12.0 XC and later releases in this and additional release trains |
| PAD Subaddressing | 12.0 XC and later releases in this and additional release trains |
| PPPoE Termination Support on Cable Interfaces | 12.1(5)T and later releases in this and additional release trains |
| Transparent LAN Services (TLS) and L2 Tunneling ATM/SIDs | 12.3(9a)BC and later 12.3 BC releases |
| VPDN MIB and Syslog Facility | 12.0 XC and later releases in this and additional release trains |
| X.25 Enhancements | 11.3(11)NA and later releases in additional release trains |
| X.25 Switching Between PVCs and SVCs | 11.3(11)NA and later releases in additional release trains |

For feature comparisons between multiple releases, refer to the corresponding release notes, or to the *Cisco IOS Feature Navigator* on Cisco.com (registration required).

# Cisco uBR7200 Series Router Configuration Tools

The Cisco uBR7200 series router provides you with the following configuration tools, allowing you flexibility in choosing your configuration method:


- Autoinstall, page 1-31
- Cable Interface Setup Facility, page 1-31
- Cable Interface Extended Setup Facility, page 1-31
- Cisco Network Registrar, page 1-32
- Interface Range Specification, page 1-32
- Internal Modem Configuration File Editor, page 1-32
- Manual Configuration Mode for the Cisco uBR7200 Series CMTS, page 1-32
- Virtual Interface Support and Frequency Stacking Support, page 1-32


## Autoinstall

The AutoInstall Using DHCP for LAN Interfaces feature replaces the use of the Bootstrap Protocol (BOOTP) with the use of the Dynamic Host Configuration Protocol (DHCP) for Cisco IOS AutoInstall over LAN interfaces. AutoInstall is a Cisco IOS software feature that provides for the configuration of a new routing device automatically when the device is initialized. DHCP (defined in RFC 2131) is based on the Bootstrap Protocol, which provides the framework for passing configuration information to hosts on a TCP/IP network. DHCP adds the capability of automatic allocation of reusable network addresses and additional configuration options.

In Cisco IOS Release 12.1(5)T, the IP address procurement phase of the AutoInstall process is now accomplished using DHCP for Ethernet, Token Ring, and FDDI interfaces. Before this release, IP addresses for LAN interfaces were obtained using BOOTP during the AutoInstall process. The AutoInstall Using DHCP for LAN Interfaces feature also allows the routing device to recognize IP address allocation messages coming from regular BOOTP servers, providing a seamless transition for those devices already using BOOTP servers for AutoInstall. Additionally, this feature allows for the uploading of configuration files using unicast Trivial File Transfer Protocol (TFTP).

Use the Autoinstall facility to configure the Cisco uBR7200 series router automatically *after* connection to your WAN. For further details, refer to these sections or documents:

- "Configuring the Cisco uBR7200 Series Using AutoInstall" section on page 2-10
- *Autoinstall Using DHCP for LAN Interfaces on Cisco.com*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt_dhcpa.htm

## Cable Interface Setup Facility

Use the Setup facility *prior to* completing a WAN or LAN connection to your router. The Setup facility supports a number of functions so that cable interfaces and cable interface line cards are fully operational after initial setup. Refer to the "Configuring the Cisco uBR7200 Series Using the Setup Facility" section on page 2-17.

## Cable Interface Extended Setup Facility

The Extended Setup facility enhances the Setup Facility by prompting you to configure each interface on the system as you progress through the CMTS configuration. The Configuration mode allows you to configure the Cisco uBR7200 series router manually if you prefer not to use Autoinstall or the Setup Facility. Refer to the "Configuring the Cable Interface with the Extended Setup Facility" section on page 2-25.

## Cisco Network Registrar

The Cisco Network Registrar (CNR) is a configuration tool that automates dynamic IP address allocation to cable interfaces, PCs, and other devices on the broadband network. CNR allows you to track serial numbers and MAC addresses for each cable interface on your network, and reduces customer service involvement when tracking subscriber CPE equipment.

Cisco provides the CNR with each Cisco uBR7200 series router. CNR dramatically improves the reliability of naming and addressing services for enterprise and service provider networks. CNR provides scalable Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) services and forms the basis of a DOCSIS cable modem provisioning system.

For additional information about configuring or using CNR, refer to the document titled *Cisco Network Registrar for the Cisco uBR7200 Series Routers*:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cabregst/6126inst.htm

## Interface Range Specification

The Interface Range Specification feature allows specification of a range of interfaces to which subsequent commands are applied and supports definition of macros that contain an interface range.

Implement the Interface Range Specification feature with the **range** keyword, which is used with the **interface** command. In the interface configuration mode with the range keyword, all entered commands are applied to all interfaces within the range until you exit interface configuration mode.

For additional command information, refer to the *Interface Range Specification* feature module on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/range.htm

## Internal Modem Configuration File Editor

This feature adds support for internal DOCSIS cable modem configuration file storage and generation. The cable modem configuration file is generated and stored as part of the Cisco IOS configuration file. The DOCSIS configuration files are not stored in Flash memory but are automatically generated when requested for TFTP downloads to cable modems.

For the latest additional information about DOCSIS configuration files, refer to the document titled *Internal DOCSIS Configurator File Generator for the Cisco Cable Modem Termination System* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufgcfile.htm

## Manual Configuration Mode for the Cisco uBR7200 Series CMTS

The Configuration mode allows you to configure the Cisco uBR7200 series router manually if you prefer not to use Autoinstall or the Setup Facility. Refer to the "Configuring the Cisco uBR7200 Series Manually Using Configuration Mode" section on page 2-27.

## Virtual Interface Support and Frequency Stacking Support

Cisco IOS Release 12.3(9a)BC supports virtual interfaces and frequency stacking on the Cisco uBR7246VXR router. Virtual interfaces allows a DS interface to be configured with up to eight upstream channels. Frequency stacking allows two frequencies to be configured on one physical connector.

For additional information about frequency stacking and virtual interfaces on the Cisco uBR7246VXR router, refer to the following document on Cisco.com:

- *Virtual Interfaces and Frequency Stacking Configuration on MC5x20S and MC28U Linecards*

  http://www.cisco.com/warp/public/109/virtual_int_freq_stack.html

# Bandwidth Management Features

This section describes the following bandwidth management feature available on the Cisco uBR7200 Series:

- Load Balancing Support, page 1-33

## Load Balancing Support

Cisco IOS Release 12.3(9a)BC introduces support for Load Balancing on the Cisco uBR7246VXR router. The Load Balancing feature allows system operators to distribute cable modems across radio frequency (RF) downstreams and upstreams, to maximize bandwidth and usage of the cable plant.

The Load Balancing feature allows service providers to optimally use both downstream and upstream bandwidth, enabling the deployment of new, high-speed services such as voice and video services. This feature also can help reduce network congestion due to the uneven distribution of cable modems across the cable network and due to different usage patterns of individual customers.

By default, the Cisco CMTS platforms use a form of load balancing that attempts to equally distribute the cable modems to different upstreams when the cable modems register. You can refine this form of load balancing by imposing a limit on the number of cable modems that can register on any particular upstream, using the **cable upstream admission-control** command.

However, this default form of load balancing affects the cable modems only when they initially register with the Cisco CMTS. It does not dynamically rebalance the cable modems at later times, such as when they might change upstream channels in response to RF noise problems, or when bandwidth conditions change rapidly because of real-time traffic such as Voice over IP (VoIP) and video services. It also does not affect how the cable modems are distributed among downstream channels.

For additional information about configuring Load Balancing on the Cisco CMTS, refer to the following document on Cisco.com:

- *Configuring Load Balancing for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a00801b17f2.html

# Cisco IOS Command-Line Enhancements

In addition to new or enhanced commands that tie to a specific feature, this section describes general enhancements to Cisco IOS Software commands that support the Cisco uBR7200 series.

- exec prompt timestamp Command, page 1-33
- parser cache Command, page 1-34
- show Command Enhancements, page 1-35
- Cisco IOS Release 12.3(9a)BC Command-Line Interface (CLI) Enhancements, page 1-36

In some cases, additional feature descriptions that relate to these commands are available elsewhere in this chapter.

## exec prompt timestamp Command

Cisco IOS Release 12.1(12c)EC and 12.2(8)BC2 add a new command, **exec prompt timestamp**. This command adds load information and a timestamp to all **show** commands. This can be useful for troubleshooting and system analysis.

The **exec prompt timestamp** command has the following syntax in line configuration mode:

```
Router(config-line)# [no] exec prompt timestamp
```

The command has the following syntax in User EXEC mode, so that users who do not know the **enable** password can also timestamp their **show** commands:

```
Router> terminal [no] exec prompt timestamp
```

The following example illustrates how to enable and disable the timestamp for the console connection:

```
Router# config t
Router(config)# line console 0
Router(config-line)# exec prompt timestamp
Router(config-line)# no exec prompt timestamp
```

The following example illustrates how to enable and disable the timestamp for the first five telnet connections:

```
Router(config)# line vty 0 4

Router(config-line)# exec prompt timestamp

Router(config-line)# no exec prompt timestamp
```

The following example illustrates how to enable and disable the timestamp when logged into User EXEC mode:

```
Router> terminal exec prompt timestamp

Router> terminal no exec prompt timestamp
```

## parser cache Command

A new global configuration command, [**no**] **parser cache**, allows you to enable or disable the parser cache feature on the Cisco uBR7200 series.The parser cache feature is enabled by default on all platforms using Cisco IOS Release 12.1(5)T or later.

The parser cache feature optimizes the parsing (translation) of Cisco IOS software configuration command lines by remembering how to parse recently encountered command lines. This feature improves the scalability of the Cisco IOS software command-line interface (CLI) parser when processing large configuration files.

This improvement is especially useful for those cases in which thousands of virtual circuits must be configured for interfaces, or hundreds of access control lists (ACLs) are required. The parser chain cache can rapidly recognize and translate configuration lines that differ slightly from previously used configuration lines (for example, pvc 0/100, pvc 0/101, and so on).

Note Testing indicates an improvement to load time of between 30% and 36% for large configuration files when using the parser cache.

For additional information, refer to the *Parser Cache* feature module on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt5parse.htm

## show Command Enhancements

The Cisco uBR7200 series universal broadband routers contain the following additional or changed **show** commands.

### show cable qos

The **show cable qos** command is changed to **show cable qos profile** *n* command, where the optional argument *n* can be used to display a specific profile.

Note The release notes up to and including Cisco IOS Release 12.0(12)SC stated that the show cable qos command was changed to **show cable qos-profile** *n* command, with a hyphen between "qos" and "profile". This was incorrect.

### show int cx/y sid

The **show int cx/y sid** command displays more complete Service ID (SID) status information.

### show cable modem

The **show cable modem** command displays a list of options for a single modem to be specified by entering either the cable modem's IP address or MAC address.

### show cable modulation-profile

The **show cable burst-profile** command has been removed. Its functions have been incorporated into the **show cable modulation-profile** command, which includes an added option number that displays the modulation profile number.

### show cable modem summary

Commencing with Cisco IOS Release 12.1(6) EC, the **show cable modem summary** command is enhanced with the following options to display per-card and per-port totals:

- **show cable modem summary total**—Displays a summary and a total for all modems on the chassis.
- **show cable modem summary** *cable x/0* **total**—Displays a summary of modems on a specified card.
- **show cable modem summary** *cable x/0* **upstream** *port1 port2* **total**—Displays a summary of modems on the specified card and specified range of ports.
- **show cable modem summary cable** *x/0 cable y/0* **total**—Displays a summary of modems on the specified range of cards.
- **show cable modem summary cable** *x/0 cable y/0* **upstream** *port1 port2* **total**—Displays a summary of modems on the specified range of ports on the specified range of cards.

For additional command information, refer to the *Cisco Broadband Cable Command Reference Guide* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/

## Cisco IOS Release 12.3(9a)BC Command-Line Interface (CLI) Enhancements

Cisco IOS Release 12.3(9a)BC supports the following new or enhanced command-line interface:


- cable logging layer2events, page 1-36
- cable source-verify, page 1-37
- show cable tech-support, page 1-41
- show controllers cable, page 1-42
- show tech-support, page 1-44


For additional information about these command changes, refer to this document on Cisco.com:

- *Cisco Broadband Cable Command Reference Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm

### cable logging layer2events

To save DOCSIS events that are specified in Cable Device MIB to the cable logging buffer (instead of to the general logging buffer), use the **cable logging layer2events** command in global configuration mode. To disable the logging of DOCSIS events to the cable logging buffer, use the **no** form of this command.

**cable logging layer2events**

**no cable logging layer2events**

#### Syntax Description

This command has no additional arguments or keywords.

#### Defaults

DOCSIS events are saved to the general logging buffer on the Cisco CMTS by default.

#### Command Modes

Global configuration mode

#### Command History

| Release | Modification |
|---|---|
| 12.3(9a)BC | This command was introduced on the Cisco uBR10012 and Cisco uBR7246VXR universal broadband routers. |

#### Usage Guidelines

Use the **show cable logging** command to check whether the logging feature is enabled and the status of the logging buffer.

#### Examples

The following example shows how to clear the log buffer that contains a bad IP source address error messages:

```
Router# show cable logging summary

Cable logging: BADIPSOURCE Enabled
Total buffer size (bytes): 1000000
```

```
Used buffer size (bytes) : 36968
Logged messages : 231

Router# clear cable logging badipsource

Router# show cable logging summary

Cable logging: BADIPSOURCE Enabled
Total buffer size (bytes): 1000000
Used buffer size (bytes) : 0
Logged messages : 0
```

Related Commands

| Command | Description |
|---|---|
| **cable logging badipsource** | Logs error messages about bad IP source addresses on the cable interfaces to a separate log buffer, |
| **show cable logging** | Indicates whether the logging feature is enabled and the status of the logging buffer. |

For additional information about logging events on the Cisco CMTS, refer to the following document on Cisco.com:

- *Cisco Broadband Cable Command Reference Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm

## cable source-verify

To enable verification of IP addresses or service IDs (SIDs) for CMs and CPE devices on the upstream, use the **cable source-verify** command in global configuration, cable interface configuration or subinterface configuration modes. To disable verification, use the **no** form of this command.

### Cable Interface and Subinterface Configuration Modes

**cable source-verify** [**dhcp** | **leasetimer** *value* | **leasequery-filter upstream** *query-num interval*]

**no cable source-verify**

### Global Configuration Mode

**cable source-verify leasequery-filter downstream** *query-num interval*

**no cable source-verify**

## Syntax Description

| | |
|---|---|
| **dhcp** | (Optional) Specifies that queries will be sent to verify unknown source IP addresses in upstream data packets.<br>Note Do not enable the local DHCP server on the Cisco CMTS and configure local DHCP address pools, using the **ip dhcp pool** command, when using this option, because this prevents DHCP address validation. |
| **leasetimer** *value* | (Optional) Specifies the time, in minutes, for how often the router should check its internal CPE database for IP addresses whose lease times have expired. The valid range for value is 1 to 240 minutes, with a default of 60 minutes.<br>Note The **leasetimer** option takes effect only when the **dhcp** option is also used on an interface. Also, this option is supported only on the master interface and cannot be configured on subinterfaces. Configuring it for a master interface automatically applies it to all subinterfaces. |
| **leasequery-filter upstream** *query-num interval* | (Optional) Enables upstream lease queries to be defined on a per-SID basis to reduce the chance of Denial of Service attacks.<br>• *query-num*— Number of leased queries per SID.<br>• *interval*—Size of timer window in seconds. |
| **leasequery-filter downstream** *query-num interval* | (Optional) Enables downstream lease queries to be defined on a per-SID basis to reduce the chance of Denial of Service attacks.<br>• *query-num*— Number of leased queries for an unknown SID.<br>• *interval*—Size of timer window in seconds. |

## Defaults

Disabled. When the **dhcp** option is specified, the **leasetimer** option is set by default to 60 minutes.

## Command Modes

Global configuration, Cable interface configuration or subinterface configuration

Note Configuring the **cable source-verify** command on the master interface of a bundle will configure it for all of the slave interfaces in the bundle as well.

## Command History

| Release | Modification |
|---|---|
| 11.3 XA | This command was introduced. |
| 12.0(7)T | The **dhcp** keyword was added. |
| 12.0(10)SC, 12.1(2)EC | Support was added for these trains. |
| 12.1(3a)EC | Subinterface support was added. |
| 12.1(13)EC, 12.2(11)BC1 | The **leasetimer** keyword was added. |
| 12.2(15)BC1 | The verification of CPE devices was changed when using the **dhcp** keyword. |

| Release | Modification |
|---|---|
| 12.2(15)BC2 | Support for verifying CMs and CPE devices that are on a different subnet than the cable interface was enhanced to use Reverse Path Forwarding (RFP). |
| 12.3(9a)BC | In order to protect the Cisco CMTS from denial of service attacks, Cisco IOS Release 12.3(9a)BC adds the option of using a per SID basis for deriving lease queries from CPE devices. This release also introduces a global rate limit for lease queries initiated by downstream traffic. These enhancements reduce the CPU utilization of DHCP Receive and ISR processes when the Cisco CMTS is configured with the **cable source-verify dhcp** and **no cable arp** commands. |

For additional information about this and other commands, refer to the following document on Cisco.com:

- *Cisco Broadband Cable Command Reference Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm

## cable submgmt default

To enable the Cisco CMTS Static CPE Override feature on the Cisco CMTS, use the **cable submgmt default** command in global configuration mode. This command enables field technicians to add a temporary CPE device behind the subscriber's cable modem. The temporary CPE device shares the same SID settings as the original CPE device, even though the temporary CPE device has a different MAC address. The original CPE device automatically changes from *dhcp cpe* to *static cpe* in the CMTS host routing tables, and the CPE device continues to receive service with the same SID. To disable Cisco CMTS Static CPE Override on the Cisco CMTS, use the **no** form of this command. This automatically updates the routing tables and enables the MAC address from the technician's laptop for a future field service connection at a different location.

**cable submgmt default** {**active** | **filter-group** {**cm** | **cpe**} | **learnable** | **max-cpe**}

**no cable submgmt default**

### Syntax Description

| | |
|---|---|
| **active** | Keyword enables Cisco CMTS Static CPE Override, granting local CPE control for subscriber management filtering (as defined by existing SID settings). |
| **filter-group** {**cm** \| **cpe**} | Keyword enables one ore more temporary CPE devices to inherit the characteristics of an existing filter group, either on the downstream or the upstream of the cable modem (**cm**) or the CPE device (**cpe**).<br>• **filter-group cm {downstream \| upstream}**—This keyword combination enables one or more temporary CPE devices to inherit and filter by the default downstream cable modem group, or by the default upstream cable modem group.<br>• **filter-group cpe {downstream \| upstream}**—This keyword combination enables one or more temporary CPE devices to inherit and filter by the default downstream CPE group, or by the default upstream CPE group. |

| | |
|---|---|
| **learnable** | Keyword automatically enables one or more temporary CPE devices to learn and to operate within the CPE IP address(es) in the Cisco CMTS routing table. |
| **max-cpe** | Keyword sets the maximum number of IP addresses to be permitted behind a cable modem while the Cisco CMTS Static CPE Override feature is enabled. This keyword enables multiple temporary CPE devices in the range of 0 to 1024. |

## Defaults

This command is disabled by default.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.3(9a)BC | This feature was introduced on Cisco uBR10012 and Cisco uBR7200 series universal broadband routers. |

## Usage Guidelines

Prior to using this command, the first (existing) DHCP CPE device maintains its DHCP dynamic MAC address behind the cable modem. The SID is assigned to this IP address.

However, by enabling Static CPE override, you gain the following states and options on two CPE devices behind the cable modem.

- The SID definition on the first CPE device is assigned a different static IP address. This enables you to change the existing (dynamic) DHCP IP address to a static IP address without first clearing the DHCP CPE host entries from the Cisco CMTS. The CPE IP state changes from **dhcp** to **static** cpe.
- This static override allows a second CPE device with a second MAC address behind the same cable modem with SID1 to be assigned same IP address as the first CPE device.

Note The second CPE device changes from **dhcp cpe** to **static CPE** in the CMTS host tables.

## Examples

The following example enables Cisco CMTS Static CPE Override in the field, enabling more or more additional CPE devices to be added behind a subscriber's cable modem:

```
Router(config)# cable submgmt default active
```

The following example configures the Cisco CMTS to accept a temporary CPE device, which inherits and filters by the subscriber's default downstream cable modem group:

```
Router(config)# cable submgmt default filter-group cm downstream
```

The following example configures the Cisco CMTS to accept a temporary CPE device, and to update the temporary CPE device with the current routing table from the Cisco CMTS:

```
Router(config)# cable submgmt default learnable
```

The following example configures the Cisco CMTS to accept a maximum of five temporary CPE devices behind a subscriber's cable modem:

```
Router(config)# cable submgmt default max-cpe 5
```

Related Commands

| Command | Description |
|---|---|
| **show cable host** | Displays the CPE devices (hosts) residing behind a specified cable modem (MAC address). |

## show cable tech-support

Cisco IOS Release 12.3(9a)BC introduces changes to the output of the **show cable tech-support** command. This change allows users with large numbers of online cable modems to collect the necessary information without consuming the console session for a long period of time.

To display general information about the router when reporting a problem, use the **show cable tech-support** command in privileged EXEC mode.

**show cable tech-support**

Syntax Description

This command has no additional arguments or keywords.

Defaults

This command has no default behavior or values.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.1(1a)T1 | This command was modified to include information about the cable clock card. |
| 12.2(15)BC2 | This command added several **show pxf** commands to the display on the Cisco uBR10012 router. |
| 12.3(9a)BC | The output of the command was significantly shortened by moving a number of **show** commands (the ones that display information about individual cable modems) to the **show tech-support** command. This release also adds support for an option to display information about only one specific cable interface. |

Examples

The following example illustrates the cable modem and interface information from a Cisco uBR7246VXR router on which Cisco IOS Release 12.3(9a)BC is installed.

```
Router# show cable tech-support
```

For additional information about this and other commands, refer to the following document on Cisco.com:

- *Cisco Broadband Cable Command Reference Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm

## show controllers cable

Cisco IOS Release 12.3(9a)BC removes the **tech-support** keyword from the **show controllers cable** command. This change allows users with large numbers of online cable modems to collect the necessary information without consuming the console session for a long period of time.

Additional and related improvements are also available for the **show tech-support** command.

To display information about the interface controllers for a cable interface on the Cisco CMTS router, use the **show controllers cable** command in user EXEC or privileged EXEC mode.

**show controllers cable** {*slot/port* | *slot*/*subslot*/*port*} [**downstream** | **upstream** [*port*] | [**mem-stat**] [**memory**] [**proc-cpu**]] [**tech-support**]

### Syntax Description

| | |
|---|---|
| *slot/port* | Identifies the cable interface and downstream port on the Cisco uBR7100 series and Cisco uBR7200 series routers.<br><br>On the Cisco uBR7100 series router, the only valid value is **1/0**. On the Cisco uBR7200 series router, *slot* can range from 3 to 6, and *port* can be 0 or 1, depending on the cable interface. |
| *slot/port* | Identifies the cable interface on the Cisco uBR7246VXR router.<br><br>Th syntax for the Cisco uBR10012 router is slot/subslot/port, where the following are the valid values:<br><br>• *slot* = 5 to 8<br>• *subslot* = 0 or 1<br>• *port* = 0 to 4 (depending on the cable interface) |
| **downstream** | (Optional) Displays downstream interface status. |
| **upstream** | (Optional) Displays upstream interface status. |
| *port* | (Optional) Specifies the desired upstream port. Valid values start with 0 for the first upstream port on the cable interface line card. |
| **mem-stat** | (Optional) Displays the output from the **show memory statistics** command to display a summary of memory statistics for a Broadband Processing Engine (BPE) cable interface line card. |
| **memory** | (Optional) Displays the output from the **show memory** command to display a summary of memory statistics, including the memory as it is allocated per process, for a Broadband Processing Engine (BPE) cable interface line card. |
| **proc-cpu** | (Optional) Displays the output from the **show processes cpu** command to display the processor status for a Broadband Processing Engine (BPE) cable interface line card. |
| **tech-support** | (Optional) Displays information from a number of different show commands for technical support purposes. The exact output depends on the platform, configuration, and type of protocols being used |

Command Modes

User EXEC, Privileged EXEC

Command History

| Release | Modification |
|---|---|
| 11.3 NA | This command was introduced. |
| 12.0(2)XC | This command was modified to show a number of additional fields. |
| 12.1(5)EC1 | Support was added for the Cisco uBR7100 series router, including information about the Cisco uBR7100 series integrated upconverter. |
| 12.2(1)XF1 | Support was added for the Cisco uBR10012 router. |
| 12.0(16)SC2,<br>12.1(10)EC1,<br>12.2(4)BC1b | The algorithm for calculating the SNR value was enhanced for a more accurate value. |
| 12.2(15)CX | Support was added for the Cisco uBR-MC28U/X cable interface line card, including the display of the number of packets dropped because they were for a Service Flow ID (SFID) of 0. |
| 12.2(15)BC2b | The **mem-stat**, **memory**, and **proc-cpu** options were added to obtain processor information from the onboard processor on Broadband Processing Engine (BPE) cable interface line cards, such as the Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, and Cisco uBR-MC5X20S/U cards. |
| 12.3(9a)BC | Adds the **tech-support** option to improve information required during technical support. |

Usage Guidelines

The **mem-stat**, **memory**, and **proc-cpu** keywords execute the related command on the processor that runs on added to obtain the relevant information from the onboard processor on Broadband Processing Engine (BPE) cable interface line cards, such as the Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, and Cisco uBR-MC5X20S/U cards. This allows you to obtain information that is specific for that particular cable interface card, as opposed to having to run these commands on the entire router.

Note The **mem-stat**, **memory**, and **proc-cpu** options are not available for cable interface line cards that do not contain an onboard processor (for example, the Cisco uBR-MC16C card).

Examples

The following is sample output for the downstream connection for slot 3 on port 0 on Cisco CMTS router from the **show controllers cable downstream** command:

```
CMTS01# show controllers cable 3/0 downstream

Cable 3/0 Downstream is up
Frequency not set, Channel Width 6 MHz, 64-QAM, Symbol Rate 5.056941 Msps
FEC ITU-T J.83 Annex A, R/S Interleave I=12, J=17
```

Table 10 describes the fields displayed by the **show controllers cable downstream** command.

*Table 10 show controllers cable downstream Field Descriptions*

| Field | Description |
|---|---|
| Cable | Slot number/port number indicating the location of the Cisco cable interface line card. |
| Downstream is up | Indicates that the RF downstream interface is enabled. |
| Frequency | Transmission frequency of the RF downstream. (This information may not match the current transmission frequency, which is external on CMTS platforms that use an external upconverter.) |
| Channel Width | Indicates the width of the RF downstream channel. |
| QAM | Indicates the modulation scheme. |
| Symbol Rate | Indicates the transmission rate (in number of symbols per second). |
| FEC ITU-T | Indicates the Motion Picture Experts Group (MPEG) framing standard. |
| R/S Interleave I/J | Indicates Reed Solomon framing based on ITU S.83-B. |

The following example illustrates the information from the **show controllers cable** command on a Cisco uBR7246VXR router on which Cisco IOS Release 12.3(9a)BC is installed.

```
Router# show controllers cable x/y
```

For additional information about this and other commands, refer to the following document on Cisco.com:

- *Cisco Broadband Cable Command Reference Guid*e

  http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm

## show tech-support

Cisco IOS Release 12.3(9a)BC shortens the output of the **show tech-support** command on the Cisco uBR10012 and the Cisco uBR7246VXR routers. This change allows users with large numbers of online cable modems to collect information without consuming the console session for a long period of time.

To display general information about the Cisco CMTS router when reporting a problem to Cisco technical support, use the **show tech-suppor**t command in privileged EXEC mode.

**show tech-support** [**page**] [**password**] [**cef** | **ipc** | **ipmulticast** | **isis** | **mpls** | ospf | **rsvp**]

Note The **show tech-support** command automatically displays the output of a number of different **show** commands. The exact output depends on the platform, configuration, and type of protocols being used.

Note The **show tech-support** includes most of the information shown in the **show cable tech-support** command.

Syntax Description

| | |
|---|---|
| **page** | (Optional) Causes the output to display a page of information at a time. Use the Return key to display the next line of output or use the space bar to display the next page of information. If not used, the output scrolls (that is, does not stop for page breaks). |
| **password** | (Optional) Leaves passwords and other security information in the output. If not used, passwords and other security-sensitive information in the output are replaced with the label "<removed>" (this is the default). |
| **cef** | (Optional) Displays information about the Cisco Express Forwarding (CEF) protocol configuration and status. |
| ipc | (Optional) Displays information about interprocess communications on the Cisco router. |
| **ipmulticast** | (Optional) Displays information about the IP multicast configuration and status. |
| **isis** | (Optional) Displays information about the Connectionless Network Service (CLNS) and Intermediate System-to-Intermediate System (IS-IS) routing protocol configuration and status.<br>Note IS-IS support is provided only on CMTS platforms running Cisco IOS images that have a “-p-” as part of the image name. |
| mpls | (Optional) Displays information about Multiprotocol Label Switching (MPLS) on the Cisco router, which instructs the routers and the switches in the network on where to forward the packets based on preestablished IP routing information. |
| ospf | (Optional) Displays information about the Open Shortest Path First (OSPF) routing algorithm and status on the Cisco router. |
| **rsvp** | (Optional) Displays information about the IP Resource Reservation Protocol (RSVP) configuration and status. |

For additional information about this and other commands, refer to the following document on Cisco.com (updated through Cisco IOS Release 12.3(9a)BC):

- *Cisco Broadband Cable Command Reference Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm

# Cisco Quality of Service Features

Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required Quality of Service (QoS) by managing delay, delay variation (jitter), bandwidth, and packet loss parameters on a network becomes the secret to a successful end-to-end business solution. Cisco QoS is the set of techniques to manage network resources. The Cisco uBR7200 series CMTS offers the following Cisco QoS features, in addition to supporting additional DOCSIS QoS features.

- Cisco Network-Based Application Recognition (NBAR), page 1-46
- RTP Header Compression, page 1-46

For additional information, refer to the *Cisco IOS Quality of Service* Web page on Cisco.com:

http://www.cisco.com/warp/public/732/Tech/qos/qos_learnabout.shtml

## Cisco Network-Based Application Recognition (NBAR)

Cisco IOS Release 12.1(10)EC added support for Cisco IOS Network-Based Application Recognition (NBAR). The NBAR feature is a new classification engine that can recognize a wide variety of network applications, including Web-based applications, client/server applications, and other difficult-to-classify protocols that dynamically assign TCP or UDP port numbers.

NBAR enhances existing methods of application-recognition by adding several new classification features:

- Classification of applications that use statically assigned TCP/UDP port numbers, that use dynamically assigned TCP/UDP port numbers, or that use protocols other than TCP and UDP
- Classification of HTTP traffic by URL, host, or MIME type
- Classification of Citrix ICA traffic by application name
- Classification of application traffic using subport information

NBAR can also classify static port protocols. Although access control lists (ACLs) can also be used for this purpose, NBAR is easier to configure and can provide other options and classification statistics that are not available when using ACLs.

After NBAR recognizes an application, the Cisco uBR7200 series router can invoke specific services appropriate for that application. These services can provide QoS features such as:

- Guaranteed bandwidth
- Bandwidth limits
- Traffic shaping
- Packet coloring

The Cisco IOS NBAR feature can also be used to detect and respond to denial-of-service and other types of network attacks. Cisco IOS NBAR uses a protocol description language module (PDLM) to define the rules by which the NBAR processes recognize an application. New PDLM definitions can usually be loaded without the need for a Cisco IOS software upgrade or a router reboot, allowing for a rapid response to discovered attacks.

Note For basic information on configuring and using the Cisco IOS NBAR feature, see the *Network-Based Application Recognition* feature module.

For information on configuring NBAR for Quality of Service (QoS) control, see the "Configuring Network-Based Application Recognition" chapter of the *Cisco IOS Release 12.2 Quality of Service Solutions Configuration Guide*.

These documents are available on Cisco.com and the Customer Documentation CD-ROM.

Tip Cisco.com also contains a technical note, *Using Network-Based Application Recognition and Access Control Lists for Blocking the Code Red Worm*, that provides information on using NBAR to block denial-of-service attacks. Registration and login is required to view this document.

## RTP Header Compression

Real-Time Transport Protocol (RTP) is the Internet Standard (RFC 1889) protocol for the transport of real-time data. It is intended to provide end-to-end network transport functions for applications that support audio, video, or simulation data over multicast or unicast network services.

RTP provides support for real-time conferencing of groups of any size within the Internet. This support includes source identification and support for gateways such as audio and video bridges as well as multicast-to-unicast translators. RTP offers QoS feedback from receivers to the multicast group, and support for the synchronization of different media streams.

RTP includes a data portion and a header portion. The data portion of RTP is a thin protocol that provides support for the real-time properties of applications, such as continuous media, including timing reconstruction, loss detection, and content identification.

The header portion of RTP is considerably large. As shown in Figure 16, the minimal 12 bytes of the RTP header, combined with 20 bytes of IP header (IPH) and 8 bytes of UDP header, create a 40-byte IP/UDP/RTP header. For compressed-payload audio applications, the RTP packet typically has a 20-byte to 160-byte payload. Given the size of the IP/UDP/RTP header combinations, it is inefficient to send the IP/UDP/RTP header without compressing it.

To avoid the unnecessary consumption of available bandwidth, the RTP header compression feature—referred to as CRTP—is used on a link-by-link basis.

For configuration information and additional explanation, refer to the "Link Efficiency Mechanisms" chapters of the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2 on Cisco.com.

# DHCP Servers and Feature Support

Cisco IOS software supports multiple DHCP features and server functions on the network for the Cisco uBR7200 series.

- Configurable Leasequery Server, page 1-47
- DHCP MAC Address Exclusion List for cable-source verify dhcp Command, page 1-48
- See the "DOCSIS 1.1 Feature Support" section on page 1-57 for additional DHCP features.

## Configurable Leasequery Server

Previously, lease query requests could only be sent to the DHCP server. Beginning with Cisco IOS Release 12.3(17a)BC, an alternate server may be configured to receive the requests.

There are a few restrictions:

- Lease queries are sent to the DHCP server unless an alternate server is configured.
- Only one alternate server may be configured.
- Users are responsible for the synchronization of the DHCP server and configured alternate server.
- If the configured alternate server fails, lease query requests will not be diverted back to the DHCP server.

Regardless of which server is configured (DHCP or alternate), unknown IP addresses that are found in packets for customer premises equipment (CPE) devices that use the cable modems on the cable interface are verified. The DHCP server or configured alternate server returns a DHCP ACK message with the MAC address of the CPE device that has been assigned this IP address, if any.

To configure the Cisco CMTS router to send DHCP LEASEQUERY requests to an alternate server, use the **cable source-verify dhcp server** *ipaddress* and **no cable arp** commands. (To configure the DHCP server instead, use the **cable source-verify dhcp** and **no cable arp** commands.)

For additional information about this feature, refer to the following documents on Cisco.com:

- *Filtering Cable DHCP Lease Queries on Cisco CMTS Routers*

  Beta URL:
  http://lbj.cisco.com/targets/ucdit/cc/td/doc/product/software/ios122/122newft/122limit/122bc/122bc_15/cblsrcvy.htm

## DHCP MAC Address Exclusion List for cable-source verify dhcp Command

Cisco IOS Release 12.3(13a)BC introduces the ability to exclude trusted MAC addresses from standard DHCP source verification checks, as supported in previous Cisco IOS releases for the Cisco CMTS. This feature enables packets from trusted MAC addresses to pass when otherwise packets would be rejected with standard DHCP source verification. This feature overrides the **cable source-verify** command on the Cisco CMTS for the specified MAC address, yet maintains overall support for standard and enabled DHCP source verification processes. This feature is supported on Performance Routing Engine 1 (PRE1) and PRE2 modules on the Cisco uBR10012 router chassis.

To enable packets from trusted source MAC addresses in DHCP, use the **cable trust** command in global configuration mode. To remove a trusted MAC address from the MAC exclusion list, use the **no** form of this command. Removing a MAC address from the exclusion list subjects all packets from that source to standard DHCP source verification.

**cable trust** *mac-address*

**no cable trust** *mac-address*

### Syntax Description

| | |
|---|---|
| *mac-address* | The MAC address of a trusted DHCP source, and from which packets will not be subject to standard DHCP source verification. |

### Usage Guidelines

This command and capability are only supported in circumstances in which the Cable Source Verify feature is first enabled on the Cisco CMTS.

When this feature is enabled in addition to cable source verify, a packet's source must belong to the MAC Exclude list on the Cisco CMTS. If the packet succeeds this exclusionary check, then the source IP address is verified against Address Resolution Protocol (ARP) tables as per normal and previously supported source verification checks. The service ID (SID) and the source IP address of the packet must match those in the ARP host database on the Cisco CMTS. If the packet check succeeds, the packet is allowed to pass. Rejected packets are discarded in either of these two checks.

Any trusted source MAC address in the optional exclusion list may be removed at any time. Removal of a MAC address returns previously trusted packets to non-trusted status, and subjects all packets to standard source verification checks on the Cisco CMTS.

For additional information about the enhanced Cable Source Verify DHCP feature, and general guidelines for its use, refer to the following documents on Cisco.com:

- *IP Address Verification for the Cisco uBR7200 Series Cable Router*

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1830/products_feature_guide09186a0080087b55.html
- *Filtering Cable DHCP Lease Queries*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a008021b8fb.html
- *Cisco Broadband Cable Command Reference Guide*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_command_reference_book09186a0080108e88.html
- CABLE SECURITY, *Cable Source-Verify and IP Address Security*, White Paper

  http://www.cisco.com/en/US/tech/tk86/tk803/technologies_tech_note09186a00800a7828.shtml

# DOCSIS 1.0 Feature Support

The Cisco uBR7200 series and associated Cisco IOS software support multiple DOCSIS 1.0 enhancements, extensions, and features.


- DOCSIS 1.0 Baseline Privacy, page 1-49
- DOCSIS 1.0 Baseline Privacy Interface Encryption and Encrypted Key Exchange, page 1-49
- DOCSIS 1.0 Concatenation Override Featurette, page 1-50
- DOCSIS 1.0 Extensions, page 1-51
- DOCSIS 1.0 Quality of Service, page 1-51
- DOCSIS Quality of Service Enhancements Prior to DOCSIS 1.1, page 1-52
- DOCSIS Customer Premises Equipment Configurator, page 1-53
- Enhanced Rate Bandwidth Allocation (ERBA) Support for DOCSIS 1.0 Cable Modems, page 1-54


## DOCSIS 1.0 Baseline Privacy

DOCSIS baseline privacy interface (BPI) gives subscribers data privacy across the RF network, encrypting traffic flows between the CMTS and cable modem. BPI ensures that a cable modem, uniquely identified by its Media Access Control (MAC) address, can obtain keying material for services only it is authorized to access.

To enable BPI, choose software at both the CMTS and cable modem that support the mode of operation. For the Cisco uBR7200 series software, choose an image with “k1” in its file name or BPI in the feature set description.

The cable modem must also support BPI. CMs must have factory-installed RSA private/public key pairs to support internal algorithms to generate key pairs prior to first BPI establishment. BPI must be enabled using the DOCSIS configuration file.

Note RSA stands for Rivest, Shamir, and Adelman, inventors of a public-key cryptographic system.

## DOCSIS 1.0 Baseline Privacy Interface Encryption and Encrypted Key Exchange

The Cisco uBR7200 series supports full DOCSIS 1.0 BPI specifications. The BPI for DOCSIS 1.0 protects user data privacy across the shared-medium cable network and prevents unauthorized access to DOCSIS-based data transport services across the cable network. BPI encrypts traffic across the RF interface between the cable modem and CMTS, and includes authentication, authorization, and accounting (AAA) features.

The level of data privacy is roughly equivalent to that provided by dedicated line network access services such as analog modems or digital subscriber lines (DSL). BPI provides basic protection of service, ensuring that a cable modem, uniquely identified by its MAC address, can obtain keying material for services only when it is authorized to access.

Note Encryption and decryption are subject to export licensing controls.

BPI supports access control lists (ACLs), tunnels, filtering, protection against spoofing, and commands to configure source IP filtering on RF subnets to prevent subscribers from using source IP addresses that are not valid.

Baseline privacy extensions permit the encryption of data transferred between the cable modem and the Cisco uBR7200 series universal broadband router. The key management protocol defined by baseline privacy allows Cisco uBR7200 series universal broadband routers to provide two types of keys to cable modems. The Key Exchange Key (KEK) decrypts the Traffic Exchange Keys (TEK). The TEK is the key used to encrypt and decrypt data packets.

## DOCSIS 1.0 Concatenation Override Featurette

Cisco IOS release 12.3(13a)BC introduces support for the DOCSIS 1.0 concatenation override feature on the Cisco uBR10012 router. This feature provides the ability to disable concatenation on DOCSIS 1.0 cable modems, even in circumstances where concatenation is otherwise supported for the upstream channel.

DOCSIS 1.0 concatenation allows the cable modem to make a single-time slice request for multiple packets, and to send all packets in a single large burst on the upstream. Concatenation was introduced in the upstream receive driver in the previous Cisco IOS releases that supported DOCSIS 1.0 +. Per-SID counters were later added in Cisco IOS release 12.1(4)CX for debugging concatenation activity.

In some circumstances, overriding concatenation on DOCSIS 1.0 cable modems may be preferable, and Cisco IOS release 12.3(13a)BC supports either option.

Note Even when DOCSIS 1.0 concatenation is disabled with this feature, concatenation remains enabled for cable modems that are compliant with DOCSIS 1.1 or DOCSIS 2.0.

To enable DOCSIS 1.0 concatenation override with Cisco IOS release 12.3(13a)BC and later releases, use the new **docsis10** keyword with the previously supported **cable upstream** <*n*> **concatenation** command in privileged EXEC mode:

**cable upstream** <*n*> **concatenation docsis10**

Syntax Description

| | |
|---|---|
| *n* | Specifies the upstream port number. Valid values start with 0 for the first upstream port on the cable interface line card. |

Examples

The following example illustrates DOCSIS 1.0 concatenation override on the Cisco uBR7246VXR router:

```
Router# no cable upstream 0 concatenation docsis10
```

In this example, DOCSIS 1.0 cable modems are updated with REG-RSP so that they are not permitted to use concatenation.

For additional information about this command, refer to the *Cisco Broadband Cable Command Reference Guide* on Cisco.com:

http://www.cisco.com/en/US/products/hw/cable/ps2217/products_command_reference_book09186a0080108e88.html

## DOCSIS 1.0 Extensions

The Cisco uBR7200 series supports the following DOCSIS 1.0 Quality of Service (QoS) extensions:

- Multi-Service ID (SID) support, allowing the definition of multiple SIDs on the upstream—Voice traffic can be designated on a higher QoS committed information rate (CIR) secondary SID, while data traffic can be forwarded on a best-effort basis on a primary SID. Secondary SIDs are higher QoS CIR-type classes that have a nonzero minimum reserved rate (CIR-type service). These SIDs receive preferential treatment at the CMTS for grants over any tiered best-effort type data SID of that upstream. Reliable operation with voice requires multiple SIDs—at least two per cable modem to separate voice from data. In DOCSIS 1.0, SIDs are set up statically. When supporting DOCSIS 1.0 extensions, SIDs can be set up statically or dynamically. Both the CMTS and cable modem must support this capability.
- Cable modem-initiated dynamic MAC messages—Dynamic Service Addition (DSA) and Dynamic Service Deletion (DSD). These messages allow dynamic SIDs to be created and deleted at run-time on a per-VoIP call basis.
- Unsolicited grant service (constant bit rate [CBR] scheduling) on the upstream—This helps provide a higher-quality channel for upstream VoIP packets from an Integrated Telephony Cable Modem (ITCM) such as the Cisco uBR924 cable access router.
- Ability to provide separate downstream rates for any given ITCM, based on the IP-precedence value in the packet—This helps separate voice signaling and data traffic that goes to the same ITCM to address rate-shaping purposes.
  - **Concatenation**—To increase the per- cable modem upstream throughput in certain releases of software, Cisco uBR7200 series software supports a concatenated burst of multiple MAC frames from a cable modem that supports concatenation.

Note All DOCSIS 1.0 extensions are activated only when a cable modem or Cisco uBR924 that supports these extensions solicits services using dynamic MAC messages or the feature set. If the CMs in your network are pure DOCSIS 1.0-based, they receive regular DOCSIS 1.0 treatment from the CMTS.

## DOCSIS 1.0 Quality of Service

The Cisco uBR7200 series universal broadband routers support quality of service (QoS) as defined by the DOCSIS 1.0 specification. Service class profiles can be configured through the command-line interface to support the QoS profile number, traffic priority, maximum upstream bandwidth, guaranteed upstream bandwidth, maximum downstream bandwidth, maximum transmit burst length, baseline privacy enable/disable, and type of service (ToS) overwrite byte.

QoS Profile Enforcement allows cable modem termination system (CMTS) operators to control the QoS to eliminate any interference from improper local-rate limiting implemented on the cable modem. The CMTS provisions a registering cable modem with a default DOCSIS 1.0 service class assigned by the operator, overriding any service class that previously existed on the modem. This service class has no upstream or downstream rate limits, so that the CMTS can do traffic shaping based on the QoS profile enforced by the operator.

The following commands are available on Cisco uBR7200 series universal broadband routers to update the QoS table:

- **create-snmp**—Permits creation of QoS table entries by SNMP.
- **modems**—Permits creation of QoS table entries by modem registration requests.
- **update-snmp**—Permits dynamic update of QoS table entries by SNMP.

## DOCSIS Quality of Service Enhancements Prior to DOCSIS 1.1

A number of DOCSIS quality of service (QoS) enhancements were added to Cisco IOS Release 12.1(1a)T1 and continue with later releases; these features paralleled some of those that were expected in the DOCSIS 1.1 specification prior to finalization.

For supported DOCSIS 1.1 QoS features, refer to the "DOCSIS 1.1 Quality of Service Features" section on page 1-60.

Note These QoS enhancements are in addition to the currently existing QoS traffic shaping and tiered best effort features.

### Concatenation Support Prior to DOCSIS 1.1

DOCSIS Concatenation combines multiple upstream packets into one packet to reduce packet overhead and overall latency, as well as increase transmission efficiency. Using concatenation, a DOCSIS cable modem needs to make only one bandwidth request for a concatenated packet, as opposed to making a different bandwidth request for each individual packet; this technique is especially effective for burst-intensive real-time traffic, such as voice calls.

Concatenation is enabled by default for current cable modem cards (see the "Cable Modem Cards" section), but can be disabled with the Cisco IOS command **no cable upstream number concatenation interface**. The **show controller** command displays whether concatenation is enabled on an interface.

Note Concatenation is supported only with cable modems that support DOCSIS concatenation.

### Embedded Client Signaling (dynamic SIDs)

Supports the dynamic creation, configuration, and deletion of Service Identifiers (SIDs) to accommodate different classes of service. This allows cable modems to request high-priority or high-bandwidth data streams as needed, such as when a VoIP call is made.

Note Dynamic SIDs can be used only with cable modems that also support this feature. Otherwise, cable modems must use the static SIDs supported in previous releases.

### IP Precedence-Based Rate Limiting

In addition to the currently supported traffic shaping techniques, Cisco IOS Release 12.1(1a)T1 supports a new configuration field that associates a maximum bandwidth (in kbps) with a particular setting of the IP type of service (ToS) bits. This can be used to ensure that certain traffic, such as data, does not exceed a preset rate limit and thereby interfere with higher-priority real-time traffic, such as VoIP calls.

### Support for Unsolicited Grants

New fields in the DOCSIS configuration file can be used so that when a cable modem requests a voice or fax SID, the MAC scheduler on the Cisco uBR7200 series router schedules fixed periodic slots on the upstream for that traffic flow. The cable modem does not have to contend for these slots, and because the Cisco uBR7200 series router controls the timing of the slots, it has a very precise control over potential delay and jitter. This provides a Constant Bit Rate (CBR) traffic flow for real-time traffic such as voice and fax calls.

In addition, the Cisco uBR7200 series router can create QoS profiles for G.711 fax traffic and G.729 voice traffic. These profiles can be customized with the scheduling parameters required for the G.711 and G.729 CODECs being used at the subscriber's site.

## DOCSIS 1.0 ToS Overwrite

Cisco IOS release 12.3(17a)BC2 introduces support for the DOCSIS 1.0 Type of Service (ToS) Overwrite feature. Currently, ToS overwrite requires the creation of static cable QoS profiles, which are then assigned to the ToS fields. This implementation works well if only a few different service types are offered. However, scalability issues arise when large numbers of service types are presented; each requiring a static QoS profile in order to perform ToS overwrite.

The Default DOCSIS 1.0 ToS Overwrite feature eliminates the need to create multiple QoS profiles in order to perform type-of-service (ToS) overwrite by automatically bounding all DOCSIS 1.0 Cable Modem (CM) created profiles to a default ToS overwrite.

## DOCSIS Customer Premises Equipment Configurator

### DOCSIS CPE Configurator V2.0.4

The DOCSIS specification requires that a DOCSIS-compliant modem download a DOCSIS configuration file during its power-on or reset sequence. This file must be in the format described in the DOCSIS Radio Frequency Specification (SP-RFI-IOS-991105).

The DOCSIS Customer Premises Equipment (CPE) Configurator V2.0.4 provides you with a Web-based graphical user interface (GUI) that allows you to collect information needed to generate and download configuration files for DOCSIS or EuroDOCSIS CMs and STBs.

There are two versions of the Cisco DOCSIS CPE Configurator V2.0.4:

- Cisco Connection Online (CCO) version (HTML-based). This Web-based, free-of-charge version needs no installation at the customer site, and is viewable at http://www.cisco.com/support/toolkit/CableModem/.
- Desktop (Java-based) version. This stand-alone, desktop version gives operators flexibility in supporting NOC and remote subscriber site usage, and is viewable at this online location:

  http://www.cisco.com/cgi-bin/tablebuild.pl/cpe-conf.

Refer to the following document for additional information about CPE Configurator V2.0.4:

- *CMTS Configuration FAQ*, Document ID: 12180

  http://www.cisco.com/warp/public/109/cable_faq_cmts_config.html

### DOCSIS CPE Configurator V3.2

Cisco has developed the DOCSIS CPE Configurator tool Version 3.2 that allows to configure DOCSIS 1.1 specific features like upstream and downstream service flows, upstream and downstream Packet Classification, and Payload Header Suppression.

If you are a registered user and are logged in to Cisco.com, you can download the stand-alone DOCSIS CPE Configurator tool Version 3.2 at this online location:

http://www.cisco.com/cgi-bin/tablebuild.pl/cpe-conf.

Refer to the following document for additional information about the DOCSIS CPE Configurator V3.2, which is available to registered, logged in users only.

- *Building DOCSIS 1.0 Configuration Files Using Cisco DOCSIS Configurator*, Document ID: 16480

  http://www.cisco.com/en/US/customer/tech/tk86/tk168/technologies_tech_note09186a0080094d00.shtml

## Enhanced Rate Bandwidth Allocation (ERBA) Support for DOCSIS 1.0 Cable Modems

Cisco IOS release 12.3(13a)BC introduces Enhanced Rate Bandwidth Allocation (ERBA) support for DOCSIS 1.0 cable modems and the Cisco uBR7200 series router. ERBA allows DOCSIS1.0 modems to burst their temporary transmission rate up to the full line rate for short durations of time. This capability provides higher bandwidth for instantaneous bandwidth requests, such as those in Internet downloads, without having to make changes to existing service levels in the QoS Profile.

This feature enables MSOs to set the DOCSIS 1.0 cable modems burst transmissions, with mapping to overriding DOCSIS 1.1 QoS profile parameters on the Cisco CMTS. DOCSIS 1.0 cable modems require DOCSIS 1.0 parameters when registering to a matching QoS profile. This feature enables maximum downstream line rates, and the ERBA setting applies to all cable modems that register to the corresponding QoS profile.

Note QoS definitions must previously exist on the Cisco CMTS headend to support this feature.

ERBA for DOCSIS 1.0 cable modems is supported with these new or enhanced commands or keywords in Cisco IOS release 12.3(13a)BC:

- **cable qos pro max-ds-burst** *burst-size*
- **show cable qos profile** *n* **[verbose]**

To define ERBA on the downstream for DOCSIS 1.0 cable modems, use the **cable qos promax-ds-burst** command in global configuration mode. To remove this ERBA setting from the QoS profile, use the **no** form of this command.

**cable qos pro max-ds-burst** *burst-size*

**no cable qos pro max-ds-burst**

Syntax Description

| | |
|---|---|
| *burst-size* | The QoS profile's downstream burst size in bytes. |

To display ERBA settings as applied to DOCSIS 1.0 cable modems and QoS profiles on the Cisco CMTS, use the **show cable qos profile** command in Privileged EXEC mode.

The following example of the **cable qos profile** command in global configuration mode illustrates changes to the **cable qos profile** command. Fields relating to the ERBA feature are shown in bold for illustration:

```
Router(config)# cable qos pro 10 ?
  grant-interval       Grant interval
  grant-size           Grant size
  guaranteed-upstream  Guaranteed Upstream
  max-burst            Max Upstream Tx Burst
  max-ds-burst        Max Downstream Tx burst (cisco specific)
  max-downstream       Max Downstream
  max-upstream         Max Upstream
  name                 QoS Profile name string (cisco specific)
  priority             Priority
  privacy              Cable Baseline Privacy Enable
tos-overwrite        Overwrite TOS byte by setting mask bits to value
```

The following example of the **show cable qos profile** command illustrates that the maximum downstream burst has been defined, and is a management-created QoS profile:

```
Router# show cable qos pro
ID  Prio Max       Guarantee Max        Max   TOS  TOS   Create  B     IP prec.
         upstream  upstream  downstream tx    mask value by      priv  rate
         bandwidth bandwidth bandwidth  burst                     enab  enab
1   0    0         0         0          0     0xFF 0x0   cmts(r) no    no
2   0    64000     0         1000000    0     0xFF 0x0   cmts(r) no    no
3   7    31200     31200     0          0     0xFF 0x0   cmts    yes   no
4   7    87200     87200     0          0     0xFF 0x0   cmts    yes   no
6   1    90000     0         90000      1522  0xFF 0x0   mgmt    yes   no
10  1    90000     0         90000      1522  0x1  0xA0  mgmt    no    no
50  0    0         0         96000      0     0xFF 0x0   mgmt    no    no
51  0    0         0         97000      0     0xFF 0x0   mgmt    no    no
```

The following example illustrates the maximum downstream burst size in sample QoS profile 10 with the **show cable qos prof verbose** command in privileged EXEC mode:

```
Router# show cable qos pro 10 ver
Profile Index                          10
Name
Upstream Traffic Priority              1
Upstream Maximum Rate (bps)            90000
Upstream Guaranteed Rate (bps)         0
Unsolicited Grant Size (bytes)         0
Unsolicited Grant Interval (usecs)     0
Upstream Maximum Transmit Burst (bytes) 1522
Downstreamam Maximum Transmit Burst (bytes) 100000
IP Type of Service Overwrite Mask      0x1
IP Type of Service Overwrite Value     0xA0
Downstream Maximum Rate (bps)          90000
Created By                             mgmt
Baseline Privacy Enabled               no
```

## Usage Guidelines

If a cable modem registers with a QoS profile that matches one of the existing QoS profiles on the Cisco CMTS, then the maximum downstream burst size, as defined for that profile, is used instead of the default DOCSIS QoS profile of 1522.

For example, a DOCSIS 1.0 configuration that matches QoS profile 10 in the previous examples would be as follows:

```
03 (Net Access Control)        = 1

04 (Class of Service Encodings Block)
   S01 (Class ID)              = 1
   S02 (Maximum DS rate)       = 90000
   S03 (Maximum US rate)       = 90000
   S06 (US burst)              = 1522
   S04 (US Channel Priority)   = 1
   S07 (Privacy Enable)        = 0
```

The maximum downstream burst size (as well as the ToS overwrite values) are not explicitly defined in the QoS configuration file because they are not defined in DOCSIS. However, because all other parameters are a perfect match to profile 10 in this example, then any cable modem that registers with these QoS parameters has a maximum downstream burst of 100000 bytes applied to it.

For further illustration, consider a scenario in which packets are set in lengths of 1000 bytes at 100 packets per second (pps). Therefore, the total rate is a multiplied total of 1000, 100, and 8, or 800kbps.

To change these settings, two or more traffic profiles are defined, with differing downstream QoS settings as desired. Table 11 provides two examples of such QoS profiles for illustration:

*Table 11 Sample QoS Profiles with Differing ERBA (Maximum Downstream) Settings*

| QoS Profile Setting | QoS Profile 101 | QoS Profile 102 |
|---|---|---|
| Maximum Downstream Transmit Burst (bytes) | max-burst 4000 | max-burst 4000 |
| Maximum Downstream Burst (bps) | max-ds-burst 20000 | max-ds-burst 5000 |
| Maximum Downstream Bandwidth | max-downstream 100 | max-downstream 100 |

In this scenario, both QoS profiles are identical except for the max-ds-burst size, which is set to 5000 in QoS profile 101 and 5000 in QoS profile 102.

### Optimal Settings for DOCSIS 1.0 Downstream Powerburst

DOCSIS allows the setting different token bucket parameters for each service flow, including the token bucket burst size. When burst sizes are closer to 0, QoS is enforced in a stricter manner, allowing a more predictable sharing of network resources, and as a result easier network planning.

When burst sizes are larger, individual flows can transmit information faster (lower latency), although the latency variance can be larger as well.

For individual flows, a larger burst size is likely to be better. As long as the system is not congested, a large burst size reduces the chances of two flows transmitting at the same time, because each burst is likely to take less time to transmit. However, as channel bandwidth consumption increases, it is probably that large burst traffic would exceed the thresholds of buffer depths, and latency is longer than with well shaped traffic.

For additional information about the **cable qos profile** command and configuring QoS profiles, refer to the following documents on Cisco.com:

- *Cisco Broadband Cable Command Reference Guide*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_command_reference_book09186a0080108e88.html

- *DOCSIS 1.1 for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b57f.html

## DOCSIS 1.0+ Feature Support

In response to the limitations of DOCSIS 1.0 in handling real-time traffic, such as voice calls, Cisco created the DOCSIS 1.0+ extensions to provide the more important QoS enhancements that were expected in DOCSIS 1.1. The main enhancements provide basic Voice-over IP (VoIP) service over the DOCSIS link, support for dynamic creation and teardown of flows during voice calls, support for one new unsolicited grant service (UGS) slot scheduling mechanism for voice slots, and per IP-precedence rate shaping on the downstream. In particular, the Cisco DOCSIS 1.0+ extensions include the DOCSIS 1.1 features described in this section:

- Concatenation for DOCSIS 1.0+, page 1-57
- Dynamic MAC messages, page 1-57
- Multiple SIDs per Cable Modem, page 1-57
- Separate Downstream Rates, page 1-57
- Unsolicited Grant Service (CBR-scheduling) on the Upstream, page 1-57

Refer to the following online document for additional information about DOCSIS 1.0+ support on the

Cisco uBR7200 Series:

- *Frequently Asked Questions on DOCSIS 1.0+*

  http://www.cisco.com/warp/public/109/DOCSIS1.0_faqs.html

### Concatenation for DOCSIS 1.0+

Concatenation allows a cable modem to send several packets in one large burst, instead of having to make a separate grant request for each.

Caution All DOCSIS 1.0 extensions are available only when using a cable modem (such as the Cisco uBR924 cable access router) and CMTS (such as the Cisco uBR7200 series router) that support these extensions. The cable modem activates the use of the extensions by sending a dynamic MAC message. DOCSIS 1.0 CMs continue to receive DOCSIS 1.0 treatment from the CMTS.

### Dynamic MAC messages

The Dynamic Service Addition (DSA) and Dynamic Service Deletion (DSD) messages allow dynamic SIDs to be created and deleted on demand so that the bandwidth required for a voice call can be allocated at the time a call is placed and then freed up for other uses when the call is over.

### Multiple SIDs per Cable Modem

This feature creates separate service flows for voice and data traffic. This allows the CMTS and cable modem to give higher priority for voice traffic, preventing the data traffic from affecting the quality of the voice calls.

### Separate Downstream Rates

This feature provides an ability to provide separate downstream rates for any given cable modem, based on the IP-precedence value in the packet—This helps separate voice signaling and data traffic that goes to the same ITCM to address rate shaping purposes.

### Unsolicited Grant Service (CBR-scheduling) on the Upstream

This feature helps provide a higher-quality channel for upstream VoIP packets from an Integrated Telephony Cable Modem (ITCM) such as the Cisco uBR924 cable access router.

## DOCSIS 1.1 Feature Support

DOCSIS 1.1 is the first major revision of the initial DOCSIS 1.0 standard for cable networks. Although the initial standard provided quality data traffic over the coaxial cable network, the demands of real-time traffic such as voice and video required many changes to the DOCSIS specification.

This section describes the major enhancements supported on the Cisco uBR7200 series:

- Baseline Privacy Interface Plus (BPI+), page 1-58
- Burst Profile Configuration, page 1-58
- Cable Modulation Profile Default Templates, page 1-58
- DHCP Cable Modem Host ID, page 1-59
- DHCP Client ID/Remote ID Options, page 1-59

- DHCP, Time of Day (ToD) and TFTP Servers, page 1-60
- DOCSIS 1.1 Quality of Service Features, page 1-60
- DOCSIS 1.1 Two-way Transmission (Cisco uBR7246VXR Router), page 1-65
- Downstream Channel ID, page 1-65
- Downstream Frequency Override, page 1-66
- Downstream Rate Shaping with IP Type of Service Bits, page 1-66
- Optional Upstream Scheduler Modes, page 1-66


## Baseline Privacy Interface Plus (BPI+)

Baseline Privacy Interface Plus (BPI+) is available and supported on the Cisco uBR7200 series with Cisco IOS Release 12.2(4)BC1 and subsequent BC1 releases.

DOCSIS 1.1 enhances these security features with Baseline Privacy Interface Plus (BPI+), which includes the following enhancements:

- Digital certificates provide secure user identification and authentication.
- Key encryption uses 168-bit Triple DES (3DES) encryption that is suitable for the most sensitive applications.
- 1024-bit public key with Pkcs#1 Version 2.0 encryption.
- Multicast support.
- Secure software download allows a service provider to upgrade a cable modem's software remotely, without the threat of interception, interference, or alteration.

Additional feature information and configuration guidelines are provided in *Configuring DOCSIS Baseline Privacy Interface on the Cisco uBR7200 Series*, available on Cisco.com:

http://www.cisco.com/en/US/products/hw/cable/ps2217/products_configuration_guide_chapter09186a00801170db.html

## Burst Profile Configuration

For each modulation/burst profile configuration, Cisco uBR7200 series universal broadband routers support burst profile number, burst profile interval usage code, burst type, preamble length and unique word length, differential encoding enable/disable, forward error correction (FEC) correctable bytes value, FEC code word length, scrambler seed value, maximum burst size, guard time size, last code word shortened/lengthened, and scrambler enable/disable.

Note Multiple burst profiles are supported on the MC11C, MC12C, MC14C, MC16B, and MC16C cable modem cards. Only one profile is supported on the original MC11-FPGA card.

## Cable Modulation Profile Default Templates

Commencing with Release 12.1(3a)EC1 and later releases, the **cable modulation-profile** global configuration command has been enhanced with three new options that enable you to quickly create basic modulation profiles using the default values for each burst type.

To define the modulation profile, use the **cable modulation-profile** command in global configuration mode. Use the **no** form of this command to remove the entire modulation profile or to reset a particular burst to its default values.

**cable modulation-profile** *profile* {**mix** | **qam-16** | **qpsk**}

**no cable modulation-profile** *profile* {**mix** | **qam-16** | **qpsk**}

Syntax Description

The syntax for the new options is as follows:

| | |
|---|---|
| *profile* | Specifies the modulation profile number (1-8). |
| **mix** | Creates a default QPSK/16-QAM mix modulation profile where short and long grant bursts are sent using 16-QAM, while request, request data, initial ranging, and station maintenance bursts are sent using QPSK). The burst parameters are set to their default values for each burst type. |
| **qam-16** | Creates a default 16-QAM modulation profile, where all bursts are sent using 16-QAM. The burst parameters are set to their default values for each burst type. |
| **qpsk** | Creates a default QPSK modulation profile, where all bursts are sent using QPSK. The burst parameters are set to their default values for each burst type. |

## DHCP Cable Modem Host ID

This feature—also known as Cable Modem and Host Subnet Addressing—allows the Cisco uBR7200 series universal broadband router to set the GIADDR field of DHCPDISCOVER and DHCPREQUEST packets with a Relay IP address to help automate the provisioning of cable modems on systems that use multiple IP subnets.

To modify the GIADDR field of DHCPDISCOVER and DHCPREQUEST packets with a Relay IP address before they are forwarded to the DHCP server, use the **cable dhcp-giaddr** command in cable interface or subinterface configuration mode. To set the GIADDR field to its default, use the **no** form of this command.

**cable dhcp-giaddr** [**policy** | **primary**]

**no cable dhcp-giaddr**

Syntax Description

| | |
|---|---|
| **policy** | (Optional) Selects the control policy, so the primary address is used for CMs and the secondary addresses are used for hosts. |
| **primary** | (Optional) Always selects the primary address to be used for the GIADDR field. Primarily used for the MC16E card and Cisco uBR7100E series routers, for support of EuroDOCSIS. |

For additional command information, refer to the *Cisco Broadband Cable Command Reference Guide* on Cisco.com.

## DHCP CIient ID/Remote ID Options

This feature—also known as the Customer Premises Equipment (CPE) Limitation—allows Cisco uBR7200 series universal broadband routers to report and limit the number of CPEs that can use the cable modem to access the cable network.

Note

This feature is separate from the cable modem's ability to support multiple CPE devices. For example, depending on the Cisco IOS software release being used, Cisco uBR900 series cable access routers can support a maximum of either 3 or 254 CPE devices. Also, by default, a DOCSIS-based cable modem supports one CPE device, but this can be changed by modifying the MAX CPE parameter in the modem's DOCSIS configuration file.

## DHCP, Time of Day (ToD) and TFTP Servers

The Cisco uBR7200 series routers support onboard Dynamic Host Configuration Protocol (DHCP) servers, Time of Day (ToD) and TFTP servers. This allows the Cisco uBR7200 series routers to provide cable modems with IP address information, to supply an RFC 868-compliant time-of-day timestamp, and to download a DOCSIS configuration file, without requiring separate and external servers.

A DOCSIS-compliant cable modem requires access to three types of servers in order to successfully come online:

- The first is a DHCP server, which provides the cable modem with an IP address, a subnet mask and other IP related parameters.
- The second is an RFC868 compliant Time-of-Day Server which lets the modem know what the current time is. A cable modem needs to know the time in order to be able to properly add accurate timestamps to its event log.
- The third is a Trivial File Transfer Protocol (TFTP) server from which a cable modem is able to download a DOCSIS configuration file containing cable modem specific operational parameters.

The Dynamic Host Configuration Protocol (DHCP) is a network management features that simplifies CMTS provisioning. DHCP provides configuration parameters to Internet hosts. DHCP consists of two components:

- a protocol for delivering host-specific configuration parameters from a DHCP server to a host
- a mechanism for allocating network addresses to hosts

DHCP is built on a client/server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts. DHCP supports three mechanisms for IP address allocation:

- Automatic allocation—DHCP assigns a permanent IP address to a client.
- Dynamic allocation—DHCP assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address).
- Manual allocation—The network administrator assigns an IP address to a client and DHCP is used simply to convey the assigned address to the client.

The Cisco IOS DHCP server feature is a full DHCP server implementation that assigns and manages IP addresses from specified address pools within the router to DHCP clients. If the Cisco IOS DHCP server cannot satisfy a DHCP request from its own database, it can forward the request to one or more secondary DHCP servers defined by the network administrator.

You can configure a DHCP server in the following ways:

- You can configure the DHCP server when using the Cable Interface Setup facility. For additional information, refer to the "Configuring the Cisco uBR7200 Series Using the Setup Facility" section on page 2-17.
- You can configure DHCP services alone, or when configuring ToD and TFTP services. For additional information, refer to the chapter titled "Configuring DHCP, ToD, and TFTP Services" in the *Cisco Cable Modem Termination System Feature Guide* on Cisco.com.

## DOCSIS 1.1 Quality of Service Features

DOCSIS 1.1 modifies the DOCSIS 1.0 specification to provide better performance, in particular for real-time traffic such as voice calls. The DOCSIS 1.1 specification provides several functional enhancements over DOCSIS 1.0 coaxial cable networks.

DOCSIS 1.1 features are supported in the Cisco IOS 12.2 BC release train, with additional DOCSIS 1.1 features being supported in certain earlier Cisco IOS 12.1 EC and 12.0 SC release trains.

### Concatenation for DOCSIS 1.1

Concatenation allows a cable modem to send multiple MAC frames in the same time slot, as opposed to making an individual grant request for each frame. This avoids wasting upstream bandwidth when sending a number of very small packets, such as TCP acknowledgement packets.

You can turn concatenation on or off. For information about configuring concatenation, refer to *Configuring Concatenation on the Cisco uBR7200 Series Cable Router* on Cisco.com.

### DOCSIS 1.0 and 1.0+ Cable Modem Support

DOCSIS 1.1 cable modems can coexist with DOCSIS 1.0 and 1.0+ cable modems in the same network—the Cisco uBR7200 series provides the levels of service that are appropriate for each cable modem.

### DOCSIS 1.1 Service Flow Model

DOCSIS 1.1 offers enhanced Quality of Service (QoS) features that give priority for real-time traffic such as voice and video:

- The DOCSIS 1.0 QoS model (a Service IDs (SID) associated with a QoS profile) has been replaced with a service flow model that allows greater flexibility in assigning QoS parameters to different types of traffic and in responding to changing bandwidth conditions
- Multiple service flows per cable modem in either direction due to packet classifiers
- Support for multiple service flows per cable modem allowing a single cable modem to support a combination of data, voice, and video traffic.
- Greater granularity in QoS per cable modem in either direction, using unidirectional service flows
- Dynamic MAC messages that can create, modify, and tear-down QoS service flows dynamically when requested by a DOCSIS 1.1 cable modem

### Downstream QoS Handling Supported

Downstream QoS handling is compliant with Multimedia Cable Network System (MCNS) requirements. For additional downstream QoS feature configuration, refer to the *DOCSIS 1.1 for the Cisco uBR7200 Series Universal Broadband Routers* feature module on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200sw/index.htm

### Dynamic MAC Messages

Dynamic Service MAC messages allow dynamic signaling of QoS between the cable modem and the CMTS. These messages are DOCSIS link layer equivalents of the higher layer messages that create, tear down, and modify a service flow. These messages are collectively known as DSX messages.

The DSX state machine module on the CMTS manages the several concurrent dynamic service transactions between cable modems and the CMTS. It include state machine support for all three DOCSIS1.1 DSX MAC messages:

- Dynamic Service Add (DSA)—This message is used to create a new service flow.
- Dynamic Service Change (DSC)—This message is used to change the attributes of an existing service flow.
- Dynamic Service Deletion (DSD)—This message is used to delete an existing service flow.

For additional information, refer to the *DOCSIS 1.1 for the Cisco uBR7200 Series Universal Broadband Routers* feature module on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200sw/index.htm

### Dynamic Map-Advance

A CMTS administrator can enhance the upstream throughput from a cable modem connected to the Cisco Cisco uBR7200 series CMTS. The system employs a new algorithm that automatically tunes the lookahead time in MAPs, based on several input parameters for the corresponding upstream channel. The use of dynamic and optimal lookahead time in MAPs significantly improves the per-modem upstream throughput.

For configuration information, refer to "Configuring the Dynamic Map Advance Algorithm" section on page 5-7.

### Dynamic SID Support

For additional feature information, refer to the document titled *Cisco uBR7200 - QoS/MAC Enhancements for Voice and Fax Calls: DOCSIS 1.0+* on Cisco.com.

### Fragmentation (Layer 2)

Layer 2 fragmentation on the upstream prevents large data packets from affecting real-time traffic, such as voice and video. Large data packets are fragmented and then transmitted in the time slots that are available between the time slots used for the real-time traffic.

### Multiple SID Support

This feature consists of changes made to various **show** commands to expand service identifier (SID) information.

- The **show cable modem** command has been changed to indicate that the SID shown is the primary SID for each cable modem.
- The **show interface cable** command has been updated to include the secondary SIDs for each cable modem.

For additional information, refer to *Multiple Service ID Support for the Cisco uBR7200 Series Cable Router* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/multisid.htm

### Payload Header Suppression (PHS)

Payload Header Suppression (PHS) conserves link-layer bandwidth by suppressing unnecessary packet headers on both upstream and downstream traffic flows.

To configure PHS, refer to the "Configuring Payload Header Suppression and Restoration" section on page 3-33. For additional information about configuring these and other DOCSIS features, refer to the *DOCSIS 1.1 for the Cisco uBR7200 Series Universal Broadband Routers* feature module on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200sw/index.htm

### QoS Configuration

QoS configuration information is now included in the Cable Modem Database Manager, which is described further in the document titled *DOCSIS 1.1 for the Cisco uBR7200 Series Universal Broadband Routers* feature module on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200sw/index.htm

### QoS Profile Enforcement

This feature allows CMTS operators to override the provisioned service class of a cable modem at the time of registration with a CMTS local-static quality of service (QoS) profile. CMTS operators can control the QoS from the CMTS and eliminate any interference from improper local-rate limiting implemented on the cable modem. The CMTS provisions a registering cable modem with a default Data-over-Cable Service Interface Specifications (DOCSIS) 1.0 service class that is assigned by the operator. This service class has no upstream or downstream rate limits.

When the modem sends data upstream, it makes bandwidth requests without throttling or dropping packets because of its own rate-policing algorithm. The CMTS does traffic shaping based on the QoS profile enforced by the operator.

For configuration information, refer to the document titled *QoS Profile Enforcement for the Cisco uBR7200 Series Router* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t4/qospr124.htm

### Time-of-Day Server

The Time-of-Day (ToD) server enables the Cisco Cable Modem Termination System (CMTS) to provide a ToD server to the CMs and other customer premises equipment (CPE) devices connected to its cable interfaces. The cable modem uses the ToD server to get the current date and time to accurately time-stamp its Simple Network Management Protocol (SNMP) messages and error log entries.

The Data-over-Cable System Interface Specifications (DOCSIS) 1.0 and 1.1 specifications require that a DOCSIS cable modem or other CPE device must specify the following time-related fields in the Dynamic Host Configuration Protocol (DHCP) request it sends during its initial power-on provisioning:

- Time Offset (option 2)—Specifies the time zone for the cable modem or CPE device, as the number of seconds that the device's time stamp is offset from Greenwich Mean Time (GMT)
- Time Server Option (option 4)—Specifies one or more IP addresses for a ToD server.
- During initial provisioning, a DOCSIS cable modem or CPE device attempts to contact the ToD server. If successful, the cable device updates its onboard clock with the time offset and timestamp received from the ToD server. If a ToD server cannot be reached or if it does not respond, the cable device eventually times out and continues on with the initialization process.

For configuration information, refer to the chapter titled "Time of Day Server" in the *Cisco Cable Modem Termination System Feature Guide* on Cisco.com.

### Trivial File Transfer Protocol Server

A DOCSIS-compliant cable modem requires access to three types of servers in order to successfully come online:

- A DHCP, Time of Day (ToD) and TFTP Servers provides the cable modem with an IP address, a subnet mask and other IP related parameters.
- A Time-of-Day Server which lets the modem know what the current time is. A cable modem needs to know the time in order to be able to properly add accurate timestamps to its event log.
- A Trivial File Transfer Protocol (TFTP) server from which a cable modem is able to download a DOCSIS configuration file containing cable modem specific operational parameters. After a cable modem has attempted to contact a ToD server, it contacts a TFTP server to download a DOCSIS configuration file. If a binary DOCSIS configuration file can be copied to a Flash device on a Cisco CMTS, then the router can act as a TFTP server for that file.

For additional information, refer to the *Cable Technology Technical Tips* Web page on Cisco.com:

http://www.cisco.com/warp/public/109/

### Type/Length/Value Parser and Encoder

The Type/Length/Value (TLV) parser and encoder is a new module that handles parsing and encoding TLVs on the CMTS. All old DOCSIS1.0/1.0+ TLVs are supported. In addition, many new TLVs have been added in DOCSIS1.1, such as service flow encodings, classifier encodings, and support for PHS rules. The new TLV parser features are used by different MAC message modules.

To display the Type/Length/Value (TLV) encodings parsed by the DOCSIS 1.1 TLV parser/encoder, use the **debug cable tlvs** command in privileged EXEC mode. The **no** form of this command disables debugging output.

**debug cable tlvs**

**no debug cable tlvs**

Refer to the following documents on Cisco.com for additional information about the TLV parser/encoder:

- *Cisco Broadband Cable Command Reference Guide*
  http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/
- *DOCSIS 1.1 for the Cisco uBR7200 Series Universal Broadband Routers*
  http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200sw/index.htm
- *Cable DOCSIS 1.1 FAQs*
  http://www.cisco.com/warp/public/109/cable_faq_docsis11.shtml

### Upstream Address Verification

This feature prevents the spoofing of IP addresses. Using the CLI, administrators can determine the IP and MAC address of a given cable interface, and the SID number that shows the IP and MAC addresses of all devices learned in the cable interface's MAC table.

The CMTS verifies the source IP address against the MAC address for the cable modem. Cable modem and PC IP addresses are verified to ensure that SID and MAC addresses are consistent. A PC behind a cable interface is assigned an IP address from the DHCP server. If a user on a second PC or cable interface statically assigns the same IP address to a PC, the Cisco uBR7200 series CMTS reports this. Using customer databases, administrators can cross-reference the spoofing cable modem and PC to prevent further usage.

The **cable source-verify** [**dhcp**] command (for cable interfaces) specifies that DHCP lease query requests are sent to verify any unknown source IP address found in upstream data packets. Upstream Address Verification requires a DHCP server that supports the new LEASEQUERY message type. Cisco Network Registrar supports the LEASEQUERY message type in Cisco IOS Release 3.01(T) and later releases.

For configuration information, refer to the "Activating Cable Modem Upstream Address Verification" section on page 5-4.

### Upstream QoS Improvements

Supported QoS models for the upstream are:

- Best-effort—Data traffic sent on a non-guaranteed best-effort basis.
- Committed information rate (CIR)—Guaranteed minimum bandwidth for data traffic.
- Unsolicited grants (UGS)—Constant bit rate (CBR) traffic, such as voice, that is characterized by fixed size packets at fixed intervals.
- Unsolicited grants with activity detection (USG-AD)—Combination of UGS and RTPS, to accommodate real time traffic that might have periods of inactivity (such as voice using silence suppression). The service flow uses UGS fixed grants while active, but switches to RTPS polling during periods of inactivity to avoid wasting unused bandwidth.

For detailed information about QoS, refer to the *DOCSIS 1.1 for the Cisco uBR7200 Series Universal Broadband Routers* feature module on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200sw/index.htm

### Upstream QoS Models Supported

Supported QoS models for the upstream are as follows:

- Best effort-Data traffic sent on a non-guaranteed best-effort basis
- Committed Information Rate (CIR)—Guaranteed minimum bandwidth for data traffic
- Unsolicited Grants (UGS)—Constant bit rate (CBR) traffic, such as voice, that is characterized by fixed size packets at fixed intervals
- Real Time Polling (rtPS)—Real Time service flows, such as video, that produce unicast, variable size packets at fixed intervals
- Unsolicited Grants with Activity Detection (USG-AD)—Combination of UGS and RTPS, to accommodate real time traffic that might have periods of inactivity (such as voice using silence suppression). The service flow uses UGS fixed grants while active, but switches to RTPS polling during periods of inactivity to avoid wasting unused bandwidth.
- Enhanced time-slot scheduling mechanisms to support guaranteed delay/jitter sensitive traffic on the shared multiple access upstream link

## DOCSIS 1.1 Two-way Transmission (Cisco uBR7246VXR Router)

The Cisco uBR7200 series routers allow DOCSIS 1.1 two-way transmission of digital data and Voice over IP (VoIP) traffic over a hybrid fiber-coaxial (HFC) network. The Cisco uBR7200 series support IP routing with a wide variety of protocols and combinations of Ethernet, Fast Ethernet, Gigabit Ethernet, serial, High-Speed Serial Interface (HSSI), Packet over SONET (POS) OC-3 and OC-12c, and Asynchronous Transfer Mode (ATM) media.

## Downstream Channel ID

This feature allows all cable modems in an HFC network to identify themselves via unique downstream channel IDs instead of their downstream frequencies.

To configure the downstream channel ID, use the **cable downstream channel-id** configuration command. Use the **no** form of this command to set the downstream channel ID to its default value.

**cable downstream channel-id** ***id***

**no cable downstream channel-id**

### Syntax DescriptionS

| | |
|---|---|
| *id* | Specifies a downstream channel ID. Valid values are from 1 to 255. |

For additional information, refer to the following documents on Cisco.com:

- *Configuring Downstream Channel IDs*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t4/downchan.htm
- *Cisco Broadband Cable Command Reference Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/bbcmtscf.htm#wp1117052

## Downstream Frequency Override

Downstream frequency override allows the CMTS administrator to change the downstream frequency assigned to a cable modem, overriding the frequency set in the cable modem DOCSIS configuration file.

To enable cable downstream frequency override, use the **cable downstream override** command in cable interface configuration mode. To disable the override feature, use the **no** form of this command.

**cable downstream override**

**no cable downstream override**

For additional command information, refer to the following document on Cisco.com:

- *Cisco Broadband Cable Command Reference Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/bbcmtscf.htm#wp1080840

## Downstream Packet Classifier

This feature helps to map packets into DOCSIS service flows. The Cisco CMTS supports downstream IP packet classifiers.

## Downstream Packet Scheduler

This module controls all output packet queuing service on the downstream link of each cable interface.

## Downstream Rate Shaping with IP Type of Service Bits

Cisco uBR7200 series routers support downstream data rate shaping on a per-modem basis. The Type of Service (ToS) bits in the IP packet header can be set to specify that packet's class of service, allowing packets for certain traffic flows (such as VoIP) to be given precedence over packets for other flows (such as data).

Downstream rate shaping with ToS bits allows you to configure multiple data rates for a given modem. Also, by specifying a maximum data rate for a particular ToS, you can override the common maximum downstream data rate. Packets that contain ToS bytes that have not been configured for downstream data rates continue to use the common data rate limits.

Prior releases set the ToS bits to zero; however, with the advent of virtual private network (VPN) and QoS applications, it is desirable to copy the ToS bits when the router encapsulates the packets using generic routing encapsulation (GRE). Thus, intermediate routers between tunnel endpoints can also take advantage of QoS features such as weighted fair queuing (WFQ) and weighted random early detection (WRED).

For additional information, refer to the following document on Cisco.com:

- *Downstream Rate Shaping with TOS Bits for the Cisco uBR7200 Series Cable Router*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/tosbit.htm

## Optional Upstream Scheduler Modes

With this feature, the user is able to select either Unsolicited Grant Services (UGS) or Real Time Polling Service (rtPS) scheduling types, as well as packet-based or TDM-based scheduling. Low latency queueing (LLQ) emulates a packet-mode-like operation over the Time Division Multiplex (TDM) infrastructure of DOCSIS. As such, the feature provides the typical trade-off between packets and TDM: with LLQ, the user has more flexibility in defining service parameters for UGS or rtPS, but with no guarantee (other than statistical distribution) regarding parameters such as delay and jitter.

### Restrictions

- To ensure proper operation, Call Admission Control (CAC) must be enabled. When the Low Latency Queueing (LLQ) option is enabled, it is possible for the upstream path to be filled with so many calls that it becomes unusable, making voice quality unacceptable. CAC must be used to limit the number of calls to ensure acceptable voice quality, as well as to ensure traffic other than voice traffic.
- Even if CAC is not enabled, the default (DOCSIS) scheduling mode blocks traffic after a certain number of calls.
- Unsolicited Grant Services with Activity Detection (UGS-AD) and Non Real Time Polling Service (nrtPS) are not supported.

#### cable upstream *n* scheduling type

Use this new command to turn the various scheduling modes on or off, where *n* specifies the upstream port.

```
Router(config-if)# [no] cable upstream n scheduling type [ugs | rtps] mode [llq | docsis]
```

For additional information about scheduler enhancements on the Cisco CMTS, refer to the following documents on Cisco.com:

- *Cisco CMTS Feature Guide — Configuring Upstream Scheduler Modes on the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_book09186a008019b6bd.html
- *DOCSIS 1.1 for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b57f.html

# DOCSIS 2.0 Feature Support

This section describes DOCSIS 2.0 enhancements supported on the Cisco uBR7200 series:

- DOCSIS 2.0 A-TDMA Support, page 1-67

## DOCSIS 2.0 A-TDMA Support

Support for DOCSIS 2.0 A-TDMA on the Cisco uBR7200 series commences with Cisco IOS Release 12.2(15)CX and continues with later releases in the 12.2 CX, 12.2 BC and 12.3 BC release trains.

The Cisco uBR-MC16U/X and Cisco uBR-MC28U/X cards improve the maximum upstream bandwidth on existing DOCSIS 1.0 and DOCSIS 1.1 cable networks by providing a number of advanced PHY capabilities that have been specified by the new DOCSIS 2.0 specifications.

The DOCSIS 2.0 A-TDMA Support feature incorporates the following advantages and improvements of DOCSIS 2.0 networks:

- Builds on existing DOCSIS cable networks by providing full compatibility with existing DOCSIS 1.0 and DOCSIS 1.1 cable modems. (The registration response (REG-RSP) message contains the DOCSIS version number to identify each cable modem's capabilities.)
- Upstreams can be configured for three different modes to support different mixes of cable modems:
  - An upstream can be configured for TDMA mode to support only DOCSIS 1.0 and DOCSIS 1.1 cable modems.
  - An upstream can be configured for A-TDMA mode to support only DOCSIS 2.0 cable modems.

– An upstream can be configured for a mixed, TDMA/A-TDMA mode, to support both DOCSIS 1.0/DOCSIS 1.1 and DOCSIS 2.0 cable modems on the same upstream.

Note DOCSIS 2.0 A-TDMA cable modems will not register on a TDMA upstream if an A-TDMA or mixed upstream exists in the same MAC domain, unless the CMTS explicitly switches the cable modem to another upstream using an Upstream Channel Change (UCC) message. DOCSIS 1.0 and DOCSIS 1.1 cable modems cannot register on an A-TDMA only upstream.

- A-TDMA mode defines new interval usage codes (IUC) of A-TDMA short data grants, long data grants, and Unsolicited Grant Service (UGS) grants (IUC 9, 10, and 11) to supplement the existing DOCSIS 1.1 IUC types
- Increases the maximum channel capacity for A-TDMA upstreams to 30 Mbps per 6 MHz channel.
- A-TDMA and mixed modes of operation provide higher bandwidth on the upstream using new 32-QAM and 64-QAM modulation profiles. In addition, an 8-QAM modulation profile is supported.
- Supports a minislot size of 1 tick for A-TDMA operations.
- Increases channel widths to 6.4 MHz (5.12 Msymbol rate).

For additional information on DOCSIS 2.0 A-TDMA Support on the Cisco uBR-MC16U/X card, refer to the section, "DOCSIS 2.0 A-TDMA Support" in *Configuring the Cisco uBR-MC16U/MC16X Cable Interface Line Card* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122cy/122c x_15/mc16uxfm.htm

For additional information on DOCSIS 2.0 A-TDMA Support on the Cisco uBR-MC28U/X card, refer to the section, "DOCSIS 2.0 A-TDMA Support" in *Configuring the Cisco uBR-MC28U/MC28X Cable Interface Line Card* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122cy/122cx_15 /mc28uxfm.htm

# High Availability Features

Several powerful High Availability features are supported on the Cisco uBR7200 series:

- Cisco DDC (Dual DOCSIS Channel), page 1-69
- DRP Server Agent, page 1-69
- DSX Messages and Synchronized PHS Information, page 1-69
- Globally Configured HCCP 4+1 Redundancy on the Cisco uBR7246VXR Router, page 1-70
- HCCP Support for the Cisco uBR-MC16S Cable Interface Line Card, page 1-70
- HCCP N+1 Redundancy, page 1-71
- High Availability Features in Cisco IOS Release 12.3(13a)BC, page 1-71
- High Availability Support for Encrypted IP Multicast, page 1-71
- Hot-Standby 1+1 Redundancy, page 1-72
- IF Muting for HCCP N+1 Redundancy, page 1-72

## Cisco DDC (Dual DOCSIS Channel)

The Cisco Dual DOCSIS Channel (DDC) feature provides redundancy to cable voice and data customers by using two or three CMTSs with connected RF upstreams and downstreams. Redundancy is provided by controlling each CMTS on which the cable modems register, and by allowing movement of the cable modems between the Cisco CMTS systems.

Cisco DDC provides redundancy during planned downtime, especially during software upgrades, with minimal configuration or control external to the Cisco CMTS.

For information about configuring, maintaining and troubleshooting DDC on the Cisco uBR7246VXR router, refer to the section "Configuring Dual DOCSIS Channel on the Cisco uBR7246VXR Universal Broadband Router" in the following document on Cisco.com:

- *Cisco Dual DOCSIS Channel (DDC) on the Cisco uBR7246VXR Universal Broadband Router*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a008026d9d5.html

## DRP Server Agent

The Director Response Protocol (DRP) is a simple User Datagram Protocol (UDP)-based application developed by Cisco Systems. It enables Cisco's DistributedDirector product to query routers (DRP Server Agents) in the field for Border Gateway Protocol (BGP) and Interior Gateway Protocol (IGP) routing table metrics between distributed servers and clients. DistributedDirector, a separate standalone product, uses DRP to transparently redirect end-user service requests to the topologically closest responsive server. DRP enables DistributedDirector to provide dynamic, scalable, and "network intelligent" Internet traffic load distribution between multiple geographically dispersed servers.

DRP Server Agents are border routers (or peers to border routers) that support the geographically distributed servers for which DistributedDirector service distribution is desired. Note that, because DistributedDirector makes decisions based on BGP and IGP information, all DRP Server Agents must have access to full BGP and IGP routing tables. For configuration information, refer to the section titled "Configuring a DRP Server Agent" in the *Cisco IOS IP Configuration Guide*, Release 12.2.

## DSX Messages and Synchronized PHS Information

Cisco IOS Release 12.3(17a)BC introduces support for PHS rules in a High Availability environment. In this release, and later releases, PHS rules synchronize and are supported during a switchover event of these types:

- Route Processor Redundancy Plus (RPR+), with Active and Standby Performance Routing Engines (PREs)
- HCCP N+1 Redundancy, with Working and Protect cable interface line cards

For additional information about these enhancements, and related High Availability features, refer to the following documents on Cisco.com:

- *N+1 Redundancy for the Cisco Cable Modem Termination System*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008015096c.html

- *Route Processor Redundancy Plus for the Cisco uBR10012 Router*

  http://www.cisco.com/en/US/products/hw/cable/ps2209/products_feature_guide09186a00801a24e0.html

## Globally Configured HCCP 4+1 Redundancy on the Cisco uBR7246VXR Router

Cisco IOS Release 12.3(17a)BC introduces support for HCCP 4+1 Redundancy on the Cisco uBR7246VXR router. Global configuration makes this High Availability feature quick to implement in the HCCP redundancy scheme.

In this High Availability configuration, four Working router chassis are supported with one Protect router chassis. These five routers are further cabled and configured with two Cisco RF Switches in the same rack using the Cisco Hot Standby Connection to Connection (HCCP) protocol.

HCCP 4+1 Redundancy is a global configuration for all the Cisco uBR7246VXR routers in the scheme. HCCP 4+1 Redundancy supports the Cisco uBR-MC28U broadband processing engine (BPE), configured in inter-chassis protection, where the Working and Protect cable interface line cards or BPEs are operating in different router chassis. A switchover event applies to an entire cable interface line card.

Note 4+1 Redundancy on the Cisco uBR7246VXR router requires that all BPEs in the router be the same.

For additional information about HCCP 4+1 Redundancy, refer to the following document on Cisco.com:

- *N+1 Redundancy for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008015096c.html

## HCCP Support for the Cisco uBR-MC16S Cable Interface Line Card

Cisco IOS Release 12.1(7)EC adds support for the Cisco uBR-MC16S cable interface line card when used in an HCCP 1+1 redundant configuration. Previously, the Cisco uBR-MC16S card could be used in a redundant configuration only by first disabling its intelligent spectrum management features.

In Cisco IOS Release 12.1(7)EC and later releases, the Cisco uBR-MC16S card can be used as the protect cable interface or working cable interface, with either another Cisco uBR-MC16S card or a Cisco uBR-MC16C card. Table 9 shows how a switchover in each of these configurations affects the intelligent spectrum management features of the Cisco uBR-MC16S card.

*Table 1-12 Switchover Operation for a Cisco uBR-MC16C/Cisco uBR-MC16S Configuration*

| Working Cable Interface | Protect Cable Interface | Operation After Switchover |
|---|---|---|
| Cisco uBR-MC16C | Cisco uBR-MC16S | The protect card (Cisco uBR-MC16S) uses the same upstream frequency as the working card, but after the system stabilizes, the protect card begins using the intelligent spectrum management features of the Cisco uBR-MC16S card, as configured on the protect CMTS. |
| Cisco uBR-MC16S | Cisco uBR-MC16C | The protect card (Cisco uBR-MC16C) uses the same upstream frequency as the working card. If the upstream becomes unstable, the Cisco uBR-MC16C performs only blind frequency hopping. |
| Cisco uBR-MC16S | Cisco uBR-MC16S | The protect card initially uses the same upstream frequency as the working card, but after the system stabilizes, the protect card continues using the intelligent spectrum management features of the Cisco uBR-MC16S card. |

For additional information, refer to *Advanced Spectrum Management Features for the Cisco uBR-MC16S Spectrum Management Card* on Cisco.com.

Note HCCP support for the Cisco uBR-MC16S card exists only in Cisco IOS Release 12.1(7)EC or later, so you cannot use the advanced spectrum management features in Cisco IOS Release 12.1(7)CX with HCCP 1+1 redundant configuration.

## HCCP N+1 Redundancy

HCCP N+1 Redundancy is made possible with the addition of the Cisco RF Switch to your cable headend network. Together with the Cisco uBR10012 and/or the Cisco uBR7246VXR routers, the Cisco RF Switch provides a fully redundant system that enables cable operators to achieve PacketCable system availability, minimize service disruptions, and simplify operations.

HCCP N+1 Redundancy is an important step toward high availability on CMTS and telecommunications networks that use broadband media. HCCP N+1 Redundancy can help limit Customer Premises Equipment (CPE) downtime by enabling robust automatic switchover and recovery in the event that there is a localized system failure.

Beginning with Cisco IOS Release 12.2(15)BC2, HCCP N+1 Redundancy adds synchronization between HCCP Working interface configurations and those inherited upon switchover to HCCP Protect interfaces. This makes the configuration of both easier and switchover times faster.

For additional configuration information about HCCP N+1 Redundancy, refer to *HCCP N+1 Redundancy for the Cisco Cable Modem Termination System* on Cisco.com:

http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008015096c.html

## High Availability Features in Cisco IOS Release 12.3(13a)BC

Cisco IOS Release 12.3(13a)BC removes support for HCCP N+1 Redundancy on the Cisco uBR7200 series routers. Associated configuration, show, and debug commands are not supported in this release.

Note The latest release to support HCCP N+1 Redundancy for the Cisco uBR7200 Series is Cisco IOS release 12.3(9a)BC. When upgrading from this or earlier supporting Cisco IOS releases to Cisco IOS release 12.3(13a)BC, the HCCP configurations are discarded and not retained.

HCCP N+1 Redundancy for the Cisco CMTS is described for earlier releases in this and additional documents on Cisco.com:

- *N+1 Redundancy for the Cisco Cable Modem Termination System*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008015096c.html

## High Availability Support for Encrypted IP Multicast

Cisco IOS Release 12.3(17a)BC introduces support for IP Multicast streams during switchover events in a High Availability environment. This feature is supported for Route Processor Redundancy Plus (RPR+), N+1 Redundancy, and encrypted BPI+ streams.

For additional information about IP Multicast and High Availability, refer to these documents on Cisco.com:

- *Cisco CMTS Universal Broadband Router MIB Specifications Guide*

http://www.cisco.com/en/US/products/hw/cable/ps2217/products_technical_reference_chapter09186a00805fd8fb.html

- *Dynamic Shared Secret for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a00801b17cc.html

- *IP Multicast in Cable Networks,* White Paper

  http://www.cisco.com/en/US/tech/tk828/technologies_case_study0900aecd802e2ce2.shtml

- *N+1 Redundancy for the Cisco Cable Modem Termination System*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008015096c.html

## Hot-Standby 1+1 Redundancy

The Hot-Standby 1+1 Redundancy feature offers the ability to provide high system availability when configuring a Cisco uBR7200 series universal broadband router to wait in hot-standby mode to protect another Cisco uBR7200 series router in case of system failure.

The 1+1 redundancy feature is essential in a residential Voice over IP (VoIP) cable network, since it provides a three- to five-second automatic system recovery time, thus helping to eliminate “call drops” in the VoIP cable network. System failure in a non-redundancy (unprotected) deployment results in loss of all voice calls in progress as well as all voice calls in “setup” phase, because the CMTS requires human intervention to reconfigure and bring the CMTS back online.

Configuration for 1+1 redundancy takes place at the cable interface line card interface level. That is, rather than assigning an entire Cisco uBR7200 series router to support another Cisco uBR7200 series router, individual interfaces on one Cisco uBR7200 series router are configured to protect individual interfaces installed in a different Cisco uBR7200 series router.

Note 1+1 redundancy protection takes place only on an inter chassis basis. That is, you cannot protect cable interfaces on a particular CMTS with cable interfaces installed in the same chassis.

You can configure the system to switch over automatically when the interface state of a cable interface line card interface moves from “up” to “down.” Alternatively, you can manually force a switch over.

Note Ensure that the same channel ID is configured for both the active and the standby cable router.

For more information on the 1+1 redundancy feature, including information on configuration tasks and command reference, refer to the document on Cisco.com:

- *Hot-Standby 1+1 Redundancy*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121ec/121ec3/hccpfeat.htm

## IF Muting for HCCP N+1 Redundancy

Beginning with Cisco IOS Release 12.2(15)BC2a, Cisco supports IF Muting with both SNMP and non-SNMP-capable upconverters in HCCP N+1 Redundancy. IF Muting offers the following benefits:

- IF Muting for either type of upconverter significantly increases the N+1 protection schemes that are available for Cisco CMTS headends.
- IF Muting offers the additional benefit of being faster than RF Muting.

- IF Muting is enabled by default. The Cisco CMTS automatically enjoys the benefits and availability of IF Muting.

For additional information about IF Muting and configuring HCCP N+1 Redundancy, refer to the following document on Cisco.com:

- *HCCP N+1 Redundancy for the Cisco Cable Modem Termination System*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008015096c.html

# Intercept Features

The Cisco uBR7200 Series supports several intercept features through multiple Cisco IOS release trains:


- Access Control List Support for COPS Intercept, page 1-73
- Cable Monitor Enhancements, page 1-74
- COPS TCP Support for the Cisco Cable Modem Termination System, page 1-74
- Service Independent Intercept (SII) Support on the Cisco uBR7200 Series, page 1-78


## Access Control List Support for COPS Intercept

Cisco IOS Release 12.3(13a)BC introduces enhanced support for Access Control Lists (ACLs) and associated commands for the Common Open Policy Service (COPS) feature.

To configure access control lists (ACLs) for inbound connections to all COPS listener applications on the Cisco CMTS, user the **cops listeners access-list** command in global configuration mode. To remove this setting from the Cisco CMTS, us the **no** form of this command.

**cops listeners access-list** {*acl-num* | *acl-name*}

**no cops listeners access-list** {*acl-num* | *acl-name*}

### Syntax Description

| | |
|---|---|
| *acl-num* | Alphanumeric identifier of up to 30 characters, beginning with a letter that identifies the ACL to apply to the current interface. |
| *acl-name* | Numeric identifier that identifies the access list to apply to the current interface. For standard access lists, the valid range is 1 to 99; for extended access lists, the valid range is 100 to 199. |

### Additional Information

Refer also the Service Independent Intercept (SII) feature in this document. For additional information, refer to the following documents on Cisco.com:

- *Configuring COPS for RSVP, Cisco IOS Versions 12.2 and 12.3*

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800b75c9.html

- *Cable Monitor and Intercept Features for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b571.html

- *PacketCable and PacketCable Multimedia on the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b576.html

- *Cisco PacketCable Primer White Paper*

  http://www.cisco.com/en/US/netsol/ns341/ns121/ns342/ns343/networking_solutions_white_paper09186a0080179138.shtml

## Cable Monitor Enhancements

Cisco IOS Release 12.3(17a)BC introduces the following enhancements to the cable monitor feature:

- Access Control Lists are now supported on the Cisco uBR-MC5X20U/D and Cisco uBR-MC28U cable interface line cards
- Unconditional downstream sniffing now enables downstream packets to be monitored, either for MAC or data packets. This enhancement supports both DOCSIS and Ethernet packet encapsulation.

For additional information about this enhancements to the cable monitor feature, refer to the following documents on Cisco.com:

- *Cable Monitor and Intercept Features on the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b571.html

## COPS TCP Support for the Cisco Cable Modem Termination System

Cisco IOS Release 12.3(13a)BC introduces optimized support for the Common Open Policy Service (COPS) feature for the Cisco uBR7200 series routers. This feature supports two new configuration commands for enabling and setting COPS processes. The COPS feature in Cisco 12.3(13a)BC enables the following COPS functions:

### COPS DSCP Marking for the Cisco CMTS

This feature allows you to change the DSCP marking for COPS messages that are transmitted or received by the Cisco router. Differentiated Services Code Point (DSCP) values are used in Quality of Service (QoS) configurations on a Cisco router. DSCP summarizes the relationship between DSCP and IP precedence.

Cisco IOS Release 12.3(13a)BC supports this function with the **cops ip dscp** command in global configuration mode.

### COPS TCP Window Size for the Cisco CMTS

This feature allows you to override the default TCP receive window size that is used by COPS processes. This setting can be used to prevent the COPS server from sending too much data at one time.

Cisco IOS Release 12.3(13a)BC supports this function with the **cops tcp window-size** command in global configuration mode.

Note These two commands affect all TCP connections with all COPS servers.

# cops ip dscp

To specify the marking for COPS messages that are transmitted by the Cisco router, use the **cops ip dscp** command in global configuration mode. To remove this configuration, use the **no** form of this command.

**cops ip dscp** *x*

**no cops ip dscp**

## Syntax Description

| | |
|---|---|
| *x* | This value specifies the markings with which COPS messages are transmitted. The following values are supported:<br>• 0-63—DSCP value ranging from 0-63.<br>• af11—Use AF11 dscp (001010)<br>• af12—Use AF12 dscp (001100)<br>• af13—Use AF13 dscp (001110)<br>• af21—Use AF21 dscp (010010)<br>• af22—Use AF22 dscp (010100)<br>• af23—Use AF23 dscp (010110)<br>• af31—Use AF31 dscp (011010)<br>• af32—Use AF32 dscp (011100)<br>• af33—Use AF33 dscp (011110)<br>• af41—Use AF41 dscp (100010)<br>• af42—Use AF42 dscp (100100)<br>• af43—Use AF43 dscp (100110)<br>• cs1—Use CS1 dscp (001000) [precedence 1]<br>• cs2—Use CS2 dscp (010000) [precedence 2]<br>• cs3—Use CS3 dscp (011000) [precedence 3]<br>• cs4—Use CS4 dscp (100000) [precedence 4]<br>• cs5—Use CS5 dscp (101000) [precedence 5]<br>• cs6—Use CS6 dscp (110000) [precedence 6]<br>• cs7—Use CS7 dscp (111000) [precedence 7]<br>• default—Use default dscp (000000)<br>• ef—Use EF dscp (101110) |

## Defaults

- For messages transmitted by the Cisco router, the default DSCP value is 0.
- For incoming connections to the Cisco router, by default, the COPS engine takes the DSCP value used by the COPS server that initiates the TCP connection.

## Usage Guidelines

- The **cops ip dscp** command allows the Cisco router to re-mark the COPS packets for either incoming or outbound connections.
- This command affects all TCP connections with all COPS servers.
- This command does not affect existing connections to COPS servers. Once you issue this command, this function is supported only for new connections after that point in time.

## Examples

The following example illustrates the cops ip dscp command with supported command variations:

```
Router(config)# cops ip dscp ?
 <0-63>   DSCP value
 af11     Use AF11 dscp (001010)
 af12     Use AF12 dscp (001100)
 af13     Use AF13 dscp (001110)
 af21     Use AF21 dscp (010010)
 af22     Use AF22 dscp (010100)
 af23     Use AF23 dscp (010110)
 af31     Use AF31 dscp (011010)
 af32     Use AF32 dscp (011100)
 af33     Use AF33 dscp (011110)
 af41     Use AF41 dscp (100010)
 af42     Use AF42 dscp (100100)
 af43     Use AF43 dscp (100110)
 cs1      Use CS1  dscp (001000) [precedence 1]
 cs2      Use CS2  dscp (010000) [precedence 2]
 cs3      Use CS3  dscp (011000) [precedence 3]
 cs4      Use CS4  dscp (100000) [precedence 4]
 cs5      Use CS5  dscp (101000) [precedence 5]
 cs6      Use CS6  dscp (110000) [precedence 6]
 cs7      Use CS7  dscp (111000) [precedence 7]
 default  Use default dscp (000000)
 ef       Use EF   dscp (101110)
```

## Additional COPS Information

Cisco 12.3(13a)BC also supports Access Control Lists (ACLs) for use with COPS. Refer to the "Access Control List Support for COPS Intercept" section on page 1-73.

For additional information about configuring COPS on the Cisco CMTS, refer to the following documents on Cisco.com:

- *Cable Monitor and Intercept Features for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b571.html

- *Configuring COPS for RSVP*

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800b75c9.html

- *COPS for RSVP*

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800b679d.html#53452

# cops tcp window-size

To override the default TCP receive window size on the Cisco CMTS, use the **cops tcp window-size** command in global configuration mode. This setting allows you to prevent the COPS server from sending too much data at one time. To return the TCP window size to a default setting of 4K, use the **no** form of this command.

**cops tcp window-size** *bytes*

**no cops tcp window-size**

## Syntax Description

| | |
|---|---|
| *bytes* | This is the TCP window size setting in bytes. This value can range from 516 to 65535 bytes. |

## Defaults

The default COPS TCP window size is 4000 bytes.

## Usage Guidelines

This command does not affect existing connections to COPS servers. Once you issue this command, this function is supported only for new connections after that point in time.

## Examples

The following example configures the TCP window size to be 64000 bytes.

```
Router(config)# cops tcp window-size 64000
```

The following example illustrates online help for this command:

```
Router(config)# cops tcp window-size ?
 <516-65535>  Size in bytes
```

## Additional COPS Information

Cisco 12.3(13a)BC also supports Access Control Lists (ACLs) for use with COPS. Refer to the "Access Control List Support for COPS Intercept" section on page 1-73.

For additional information about configuring COPS on the Cisco CMTS, refer to the following documents on Cisco.com:

- *Cable Monitor and Intercept Features for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b571.html

- *Configuring COPS for RSVP*

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800b75c9.html

- *COPS for RSVP*

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800b679d.html#53452

## Service Independent Intercept (SII) Support on the Cisco uBR7200 Series

The Cisco CMTS supports the Communications Assistance for Law Enforcement Act (CALEA) for voice and data. Cisco IOS Release 12.3(13a)BC introduces support for Service Independent Intercept (SII) on the Cisco uBR7200 CMTS. Cisco SII provides a more robust level of the lawful intercept (LI) options offered in the Packet Intercept feature. Cisco SII is the next level of support for judicially authorized electronic intercept, to include dial access, mobile wireless, tunneled traffic, and Resilient Transport Protocol (RTP) for voice and data traffic on the Cisco CMTS.

SII on the Cisco CMTS in Cisco IOS release 12.3(13a)BC includes these functions:

- Packet intercept on specified or unspecified interfaces or ports, including port lists
- Packet intercept on virtual interface bundles
- Corresponding SNMP MIB enhancements for each of these functions, as intercept requests are initiated a mediation device (MD) using SNMPv3

Note No new CLI commands are provided for this feature in Cisco IOS release 12.3(13a)BC.

Cisco IOS Release 12.3(13a)BC enables full Multiple Service Operator (MSO) compliance with SII and LI regulations. Service providers worldwide are legally required to allow government agencies to conduct surveillance on the service provider's traditional telephony equipment. The objective of the SII feature is to enable service providers with New World networks that legally allow government agencies to conduct electronic network surveillance.

Lawful Intercept (LI) describes the process and judicial authority by which law enforcement agencies conduct electronic surveillance of circuit and packet-mode communications. LI is authorized by judicial or administrative order and implemented for either voice or data traffic on the Cisco CMTS. Table 13 lists the differences between packet intercept and SII features

*Table 13 Differences Between Packet Intercept and SII Features*

| Feature | Packet Intercept | Service Independent Intercept |
|---|---|---|
| Interface Type | Cable | Any |
| IP Masks | 255.255.255.255 or 0.0.0.0 | Any |
| L4 Ports | Any single port or 0-65535 | Any port range |
| Protocol | UDP | Any |
| TOS/DSCP | Not supported | Supported |

### Additional Information

For additional information, refer to the following documents:

- *Configuring COPS for RSVP, Cisco IOS Versions 12.2 and 12.3*

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800b75c9.html

- *Cable Monitor and Intercept Features for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b571.html

- *PacketCable and PacketCable Multimedia on the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b576.html

- *Cisco PacketCable Primer White Paper*

  http://www.cisco.com/en/US/netsol/ns341/ns121/ns342/ns343/networking_solutions_white_paper09186a0080179138.shtml

# IP Broadcast and Multicast Features

The Cisco uBR7200 Series supports the following IP broadcast and Multicast feature:

- Multicast QoS Support on the Cisco uBR7246VXR CMTS, page 1-79

## Multicast QoS Support on the Cisco uBR7246VXR CMTS

Cisco IOS Release 12.3(13a)BC introduces support for Multicast downstream QoS feature. This feature t provides the ability to assign static mapping to a multicast group. The Multicast downstream QoS feature uses the existing infrastructure (DOCSIS 1.1 service flow) to assign a multicast service identifier (SID) to a multicast group used in the Baseline Privacy Interface (BPI) encryption feature.

When disabled, the Multicast downstream QoS feature does not impact any other features. The multicast packets to downstream cable interfaces are sent to the default service flow.

This feature is being implemented in response to CSCeg22989 which states, multicast traffic is not classified to any service flow, and therefore ends up queued on the default service flow. The default service flow has no specific QoS guarantees assigned to it. So once the interface approaches congestion level, multicast packets may be dropped.

### Restrictions

- The multicast definitions are per-bundle, not per interface. This means that all downstreams in a bundle share the same multicast to QoS association. The downstreams will create their own service flows according to the same QoS parameters.
- Multicast to QoS definitions can not be assigned per sub-interface
- Multicast SIDs are not deleted when a group becomes idle (no response to IGMP reports).
- The QoS assignments for a multicast group can not be changed dynamically. If the user wishes to change them then a new “cable match” command must be configured.
- Multicast QoS is not supported on Multicast Echo on Cisco uBR10012 router.

New and Changed Commands

cable match address

Use the existing “cable match” command to assign QoS to a multicast group, with BPI either enabled or disabled.

```
router# cable match address <number>|<name> [service-class <name> [bpi-enable]]
router# no cable match address [<number>|<name> [service-class <name> [bpi-enable]]]
```

debug cable mcast-qos

Use this command to turn on CMTS Multicast Qos debugging.

```
router# debug cable mcast-qos
```

# IP Routing Features

The Cisco uBR7200 series router offers you several features to assist with IP routing configuration and performance.


- Cable ARP Filter Enhancement, page 1-80
- cable intercept Command, page 1-81
- Cable Interface Bundling and Cable Subinterfaces, page 1-82
- Configurable Alternate Termination System Information Messages, page 1-83
- Easy IP (Phase 1), page 1-83
- Fast-Switched Policy Routing, page 1-83
- IP Enhanced IGRP Route Authentication, page 1-84
- IP Network Address Translation/Port Address Translation, page 1-84
- NAT—Support for NetMeeting Directory (Internet Locator Service—ILS), page 1-84
- Router-Port Group Management Protocol, page 1-85
- Supported Protocols on the Cisco uBR7200 Series, page 1-85


## Cable ARP Filter Enhancement

The **cable arp filter** command, introduced with Cisco IOS Release 12.2(15)BC2b, enables service providers to filter ARP request and reply packets. This prevents a large volume of such packets from interfering with the other traffic on the cable network.

Cisco IOS Release 12.3(9a)BC introduces enhanced command option syntax for the **cable arp filter** command, where *number* and *window-size* values are optional for **reply-accept** and **request-send** settings.

To control the number of Address Resolution Protocol (ARP) packets that are allowable for each Service ID (SID) on a cable interface, use the **cable arp** command in cable interface configuration mode. To stop the filtering of ARP broadcasts for CMs, use the **no** form of this command.

**cable arp filter** {**reply-accept** *number window-size* | **request-send** *number window-size*}

**no cable arp filter** {**reply-accept** | **request-send**}

**default cable arp filter** {**reply-accept** | **request-send**}

Syntax Description

| | |
|---|---|
| **reply-accept** *number window-size* | Configures the cable interface to accept only the specified *number* of ARP reply packets every *window-size* seconds for each active Service ID (SID) on that interface. The cable interface drops ARP reply packets for a SID that would exceed this number.<br>• *number* = (Optional) Number of ARP reply packets that is allowed for each SID within the window time period. The allowable range is 0 to 20 packets, with a default of 4 packets. If *number* is 0, the cable interface drops all ARP reply packets. If not specified, this value uses default.<br>• *window-size* = (Optional) Size of the window time period, in seconds, in which to monitor ARP replies. The valid range is 1 to 5 seconds, with a default of 2 seconds. |
| **request-send** *number window-size* | Configures the cable interface to send only the specified *number* of ARP request packets every *window-size* seconds for each active SID on that interface. The cable interface drops ARP requests for a SID that would exceed this number.<br>• *number* = (Optional) Number of ARP request packets that is allowed for each SID within the window time period. The allowable range is 0 to 20 packets, with a default of 4 packets. If *number* is 0, the cable interface does not send any ARP request packets.<br>• *window-size* = (Optional) Size of the window time period, in seconds, in which to monitor ARP requests. The valid range is 1 to 5 seconds, with a default of 2 seconds. |

Cisco IOS Release 12.3(9a)BC also removes a prior caveat with HCCP Protect interfaces. Previously, in the event of a revert-back HCCP N+1 switchover, manual removal of **cable arp filter reply** and **cable arp filter request** configurations may have been required afterward on Protect interfaces.

For more information about ARP Filtering, refer to the following document on Cisco.com:

- *Cable ARP Filtering*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a00801eefa9.html

## cable intercept Command

Use the **cable intercept** command in cable interface configuration mode to allow the CMTS to forward all traffic to and from a particular cable modem to a data collector located at particular User Datagram Protocol (UDP) port. To deactivate this function, use the **no** form of this command.

**cable intercept** *mac-address ip-address udp-port*

**no cable intercept** *mac-address*

The **cable intercept** command can be used to comply with the United States Federal Communications Assistance for Law Enforcement Act (CALEA) and other law enforcement wiretap requirements for voice communications.

Syntax Description

| | |
|---|---|
| *mac-address* | Specifies the MAC address to be intercepted. |
| *ip-address* | Specifies the IP address for the destination data collector. |
| *udp-port* | Specifies the destination UDP port number for the intercept stream at the data collector. Valid range is 0 to 65535. |

For additional command information, refer to the *Cisco Broadband Cable Command Reference Guide*.

## Cable Interface Bundling and Cable Subinterfaces

Support for cable interface bundling on the Cisco uBR7200 series commences with Cisco IOS Release 12.2(4)XF1 and continues with later Cisco 12.2 BC releases.

To reduce the number of subnets consumed per Cisco CMTS, cable interface bundling is used. Multiple cable interfaces can share a single IP subnet. An IP subnet is required for each bundle. You can bundle all cable interfaces on a Cisco CMTS into a single bundle.

Note Cable interface bundling is applicable only in two-way cable configurations. It is not supported in telco-return configurations.

Using the CLI, first configure a master interface for a cable interface bundle. The master interface has an IP address assigned and is visible for IP routing functionality. After you configure the master interface, add additional cable interfaces to the same interface bundle. Those interfaces must not have an IP address assigned. You can also configure multiple bundle interfaces.

Use the following commands to configure and view cable interface bundles:

[**no**] **cable bundle** *n* **master**

**show cable bundle**

Up to four interface bundles can be configured. In each bundle, specify exactly one interface as the master interface, using the "master" keyword. In the case of a subinterface over a cable bundle, `x' is the interface number of the bundle master [1]. The subinterface number starts from 1.

Caution Configure an IP address on the master interface only. An attempt to add an interface to a bundle will be rejected if an IP address is configured and the interface is not specified as a master interface.

When bundling cable interfaces, only the interface configured to be the bundle master is allowed to have subinterfaces. An interface that has subinterface(s) defined over it will not be allowed to be part of a bundle. MIB objects on cable interface bundles are not supported as of the date of this publication.

For more information on cable bundling, refer to these documents on Cisco.com:

- *Cable Interface Bundling for the Cisco uBR7200 Series Cable Router* feature module:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120xr/bundling.htm

- *Bundling Cable Interfaces Sample Configuration and Verification*, TAC Document ID 44122

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_configuration_example09186a00801ae255.shtml

## Configurable Alternate Termination System Information Messages

The registration IP address that is included in Termination System Information messages is now configurable for telco return. Previously, the downstream channel IP address of the uBR7200 was used as the registration IP address.

To select a different IP address for the telco-return cable modem to send its registration requests, use the **cable telco-return registration-ip** command in cable interface configuration mode. To restore the default value, use the **no** form of this command.

**cable telco-return registration-ip** *ip-address*

**no cable telco-return registration-ip**

Syntax Description

| | |
|---|---|
| *ip-address* | Registration IP address that is sent in Termination System Information (TSI) messages. Value is any of the cable interface's IP addresses. |

For additional information about telco return and the **cable telco-return registration-ip** command, refer to these documents on Cisco.com:

- "Telephone Return for the Cisco uBR7200 Series Cable Router" chapter in the Cisco Cable Modem Termination System Feature Guide:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/telco125.htm

- *cable telco-return registration-ip Command in the Cisco Broadband Cable Command Reference Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/bbcmtscf.htm#wp1201355

## Easy IP (Phase 1)

The Easy IP (Phase 1) feature combines Network Address Translation (NAT) and point-to-point protocol (PPP)/Internet Protocol Control Protocol (IPCP). This feature enables a Cisco router to negotiate automatically its own registered WAN interface IP address from a central server and to enable all remote hosts to access the Internet using this single registered IP address. The ability of multiple LAN devices to use the same globally unique IP address is known as overloading. Because Easy IP (Phase 1) uses existing port-level multiplexed NAT functionality within the Cisco IOS software, IP addresses on the remote LAN are invisible to the Internet.

With PPP/IPCP, the Cisco uBR7200 routers automatically negotiate a globally unique (registered) IP address for the dialer interface from the ISP router. For additional information, refer to the following document on Cisco.comk:

- *Configuring Easy IP*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/dial_c/dcezip.htm

## Fast-Switched Policy Routing

IP policy routing can now be fast switched. Prior to this feature, policy routing could only be process switched, meaning that on most platforms, the switching rate was approximately 1000 to 10,000 packets per second. Such rates were not fast enough for many applications. Users that need policy routing to occur at faster speeds can now implement policy routing without slowing down the router.

Fast-switched policy routing supports all of the **match** commands and most of the **set** commands with a few restrictions. Refer to the chapter titled "Configuring IP Routing Protocol-Independent Features" in the *Cisco IOS IP Configuration Guide*, Release 12.2 on Cisco.com.

## IP Enhanced IGRP Route Authentication

The latest Interior Gateway Routing Protocol (IGRP) is an enhanced version of the IGRP developed by Cisco. Enhanced IGRP uses the same distance vector algorithm and distance information as IGRP. However, the convergence properties and the operating efficiency of Enhanced IGRP have improved significantly over IGRP.

The convergence technology is based on research conducted at SRI International and employs an algorithm referred to as the Diffusing Update Algorithm (DUAL). This algorithm guarantees loop-free operation at every instant throughout a route computation and allows all devices involved in a topology change to synchronize at the same time. Routers that are not affected by topology changes are not involved in recomputations. The convergence time with DUAL rivals that of any other existing routing protocol.

For configuration information, refer to the following document on Cisco.com:

- "Configuring IP Enhanced IGRP" chapter in the *Cisco IOS IP Routing Configuration Guide*, Release 12.2

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt2/1cfeigrp.htm

## IP Network Address Translation/Port Address Translation

Network Address Translation (NAT) is a mechanism for conserving registered IP addresses in large networks and simplifying IP addressing management tasks. As its name implies, Cisco IOS NAT translates IP addresses within private "internal" networks to "legal" IP addresses for transport over public "external" networks (such as the Internet). Incoming traffic is translated back for delivery within the inside network.

Thus, Cisco IOS NAT allows an organization with unregistered "private" addresses to connect to the Internet by translating those addresses into globally registered IP addresses. Cisco IOS NAT also increases network privacy by hiding internal IP addresses from external networks.

You can configure several internal addresses with NAT to only one or a few external addresses by using a feature called Port Address Translation (PAT) which is also referred to as "overload," a subset of NAT functionality.

PAT uses unique source port numbers on the Inside Global IP address to distinguish between translations. Because the port number is encoded in 16 bits, the total number could theoretically be as high as 65,536 per IP address. PAT will attempt to preserve the original source port, if this source port is already allocated PAT will attempt to find the first available port number starting from the beginning of the appropriate port group 0-511, 512-1023, or 1024-65535. If there is still no port available from the appropriate group and more than one IP address is configured, PAT will move to the next IP address and try to allocate the original source port again. This continues until it runs out of available ports and IP addresses.

For the first steps in configuring Network Address Translation, refer to the following document on Cisco.com:

- *"Configuring Network Address Translation: Getting Started*

  http://www.cisco.com/warp/public/556/12.html

For additional information about IP NAT and PAT, refer to the following document on Cisco.com:

- *"Product Bulletin No. 1195, Cisco IOS Network Address Translation (NAT)*

  http://www.cisco.com/warp/public/cc/pd/iosw/ioft/ionetn/prodlit/1195_pp.htm

## NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)

The Cisco IOS Network Address Translation (NAT) supports the Microsoft NetMeeting directory. Microsoft NetMeeting is a Windows-based application that enables multi user interaction and collaboration from a user's PC over the Internet or an intranet. Support for the NetMeeting Directory (ILS) allows connections by name from the directory built into the NetMeeting application. Destination IP addresses do not need to be known in order for a connection to be made.

For additional information, refer to the following document on Cisco.com:

- *NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtnatils.htm

## Router-Port Group Management Protocol

The Router-Port Group Management Protocol (RGMP) feature introduces a Cisco protocol that restricts IP multicast traffic in switched networks. RGMP is a Layer 2 protocol that enables a router to communicate to a switch (or a networking device that is functioning as a Layer 2 switch) the multicast group for which the router would like to receive or forward traffic. For additional information, refer to the following document on Cisco.com:

- *Router-Port Group Management Protocol*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s10/dtrgmp.htm

## Supported Protocols on the Cisco uBR7200 Series

The Cisco uBR7200 Series supports multiple protocols of multiple classes, including but not limited to, the following:

- Address Resolution Protocol (ARP)
- Cisco Discovery Protocol (CDP)
- Domain Name System (DNS)
- Internet Protocol (IP) v4/v5
- Simple Network Management Protocol (SNMP) v2 and SNMPv3 Integrated Dynamic Host Configuration Protocol (DHCP) server
- Trivial File Transfer Protocol (TFTP) client
- User Datagram Protocol (UDP)

Note Be aware that when configuring a routing protocol, the Cisco IOS software must reset the interfaces to enable the change. This normally does not significantly affect operations on the interface, except that when this is done on a cable interface, it causes all cable modems on that particular downstream to reinitialize, potentially interfering with data transmission on that downstream. Therefore, you should use routing global configuration commands, such as router rip, on a cable interface only when a minimum of subscribers would be affected.

For additional information about configuring IP routing protocols, refer to the following document on Cisco.com:

- "IP Routing Protocols" chapter in the *Cisco IOS IP Configuration Guide*, Release 12.2

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt2/

# Management Features

The Cisco uBR7200 series routers provide you with the following features that make CMTS headend configuration, management, and DOCSIS support more powerful and efficient:


- Admission Control for the Cisco CMTS, page 1-86
- Cable ARP and Proxy ARP, page 1-87
- cable map-advance Command Enhancements, page 1-87
- cable monitor Command, page 1-88
- Cisco IOS Internationalization, page 1-88
- DOCSIS 2.0 SAMIS ECR Data Set, page 1-88
- Dynamic Channel Change (DCC) for Loadbalancing, page 1-89
- Dynamic Ranging Support, page 1-90
- Enhanced Modem Status Display, page 1-90
- Entity MIB, Phase 1, page 1-91
- Load Balancing for the Cisco CMTS, page 1-91
- Management Information Base (MIB) Changes and Enhancements, page 1-91
- MAX-CPE Override for Cable Modems, page 1-92
- Per-Modem Error Counter Enhancements, page 1-92
- Pre-equalization Control for Cable Modems, page 1-93
- Subscriber Traffic Management (STM) Version 1.1, page 1-95
- Usage Based Billing (SAMIS), page 1-96


## Admission Control for the Cisco CMTS

Admission Control for the Cisco Cable Modem Termination System (CMTS) is a multifaceted feature that implements a Quality of Service (QoS) policy on the CMTS Headend. Admission Control establishes efficient resource and bandwidth utilization in a way that was not possible in prior Cisco IOS releases.

Admission Control monitors multiple system-level resources on the Cisco CMTS, and performs automatic resource allocation on a service-request basis. Admission Control maintains optimal system-level operation by preventing resource consumption that would otherwise degrade the performance for the entire Cisco CMTS. Furthermore, Admission Control can allocate upstream or downstream bandwidth resources to specific DOCSIS traffic types, and maintain such prioritization amidst very dynamic traffic conditions.

Admission Control uses two event types for resource monitoring and management—cable modem registration and dynamic service (voice call) requests. When either of these two events occurs on the Cisco CMTS, Admission Control verifies that the associated resources conform to the configured limits prior to admitting and supporting the service call request.

Admission Control is not a mechanism to apply QOS to the traffic flows. Scheduling and queuing are some of the mechanisms used for implementing the QOS. The QOS is applied  on per packet basis. Admission Control checks are performed before the flow is committed.

Admission Control in Cisco IOS Release 12.3(13)BC monitors the following resources on the Cisco CMTS.

- *CPU utilization*—Admission Control monitors CPU utilization on the Cisco CMTS, and preserves QoS for existing service flows when new traffic would otherwise compromise CPU resources on the Cisco CMTS.
- *Memory resource utilization (I/O, Processor, and combined total)*—Admission Control monitors one or both memory resources and their consumption, and preserves QoS in the same way as CPU utilization.
- *Bandwidth utilization for upstream and downstream*—Admission Control monitors upstream and downstream bandwidth utilization, and associated service classes, whether for data or dynamic service traffic.

Cisco IOS Release 12.3(13a)BC introduces new configuration, **debug** and **show** commands for Admission Control on the Cisco CMTS. For additional information, refer to the following document on Cisco.com:

- *Admission Control for the Cisco Cable Modem Termination System*

http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a00804d2537.html

## Cable ARP and Proxy ARP

The **cable arp** and **cable proxy-arp** commands control whether the Cisco uBR7200 series router allows ARP requests on the cable interfaces and whether the router serves as a proxy ARP server for cable modems, so that cable modems on the same subnet can communicate with each other, without having to send the traffic through the Cisco uBR7200 series router.

For additional information about these and other CMTS commands, refer to the *Cisco Broadband Cable Command Reference Guide* on Cisco.com.

## cable map-advance Command Enhancements

Cisco IOS Release 12.1(10)EC updates the **cable map-advance** command with a new option, *max-delay*. The new command syntax is the following:

**cable map-advance** [**dynamic** [*safety*] | **static**] [*max-delay*]

The *max-delay* option specifies the maximum round trip delay between the cable plant and furthest cable modem in microseconds. The valid range is 100 to 2000 microseconds. The typical delay for a mile of coaxial cable is approximately seven microseconds. The typical delay for a mile of fiber cable is approximately eight microseconds.

A cable modem will not be allowed to exceed the maximum timing offset given by the max-delay value (in static mode) or given by the combination of the max-delay and safety values (in dynamic mode). If a cable modem reports a timing offset beyond the maximum value, the CMTS will reset its offset to the maximum value and put an exclamation point (!) next to its offset value in the show cable modem display.

In dynamic MAP operation, Cisco IOS 12.1(10)EC also implements a regular polling of the furthest cable modem, to determine if that cable modem is now offline. If the furthest cable modem has gone offline, the CMTS scans the currently online CMs to determine which is now the furthest offline and updates the dynamic MAP advance algorithm with the new value.

Tip

The **show cable modem** command displays the cable modem timing offset in DOCSIS ticks. Use the following method to convert microseconds to DOCSIS ticks: ticks = microseconds*64/6.25.

## cable monitor Command

The Cisco IOS command-line interface (CLI) **cable monitor** command allows an external LAN packet analyzer on the cable interface to monitor inbound and outbound data packets for specific types of traffic between the Cisco Cable Modem Termination System (CMTS) and the CMs attached to the radio frequency (RF) line card. This feature enables the CMTS administrator to analyze traffic problems with customer data exchanges.

The **cable monitor** command specifies the set of filter criteria the CMTS uses to monitor and forward copies of data packets from a cable modem, identified by its MAC address (or access list representing a group of MAC addresses). Data packets matching the filter criteria are forwarded out of a specified Ethernet or Fast Ethernet port on the CMTS to a LAN packet analyzer. The LAN packet analyzer (sometimes called "sniffer") receives the data packets, displays the data, and stores it for analysis.

For cable monitor configuration information, refer to the following document on Cisco.com:

- "Cable Monitor and Intercept Features for the Cisco CMTS" chapter in the *Cisco Cable Modem Termination System Feature Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufg_cmon.htm

## Cisco IOS Internationalization

Your Cisco IOS platform automatically displays 8-bit and multibyte character sets and prints the ESC character as a single character instead of as the caret and bracket symbols (^[) when the Cisco Web browser interface is enabled with the **ip http server** command.

Use the **international** command in line configuration mode to display 8-bit and multibyte international character sets and print the ESC character as a single character instead of "^[" when using Telnet to access a Cisco IOS platform.

Use the **terminal international** command in privileged EXEC mode to display 8-bit and multibyte international character sets and print the ESC character as a single character instead of "^[" when using Telnet to access a Cisco IOS platform for the current session.

For information about specifying international character sets, refer to the chapter titled "Configuring Operating Characteristics for Terminals" in the *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2. To customize the user interface on a Web browser, refer to the chapter titled "Using the Cisco Web Browser User Interface" in the same guide.

## DOCSIS 2.0 SAMIS ECR Data Set

The Usage-Based Billing feature for the Cisco Cable Modem Termination System (CMTS) provides subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format. The SAMIS format is specified by the Data-over-Cable Service Interface Specifications (DOCSIS) Operations Support System Interface (OSSI) specification.

Release 12.3(17a)BC provides enhancements to the OSSI specifications, and billing reports (billing record format), added support to the CISCO-CABLE-METERING-MIB, which contains objects that provide subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format, added support for DCC and DCC for Load balancing and Downstream LLQ.

For additional information, refer to the following document on Cisco.com:

- *Usage-Based Billing for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a00801ef1d7.html

## Downstream Load Balancing Distribution with Upstream Load Balancing

Cisco IOS Release 12.3(17b)BC4 introduces further enhancements to downstream load balancing, resulting in equalized upstream load balancing group members. This enhancement synchronizes the pending statistic between different cable interface line cards in the load balancing group.

This enhancement performs downstream load balancing that accounts for loads on upstream channels in the same upstream load balancing group, rather than on the basis of the entire downstream channel load. Prior Cisco IOS releases may not have distributed cable modems evenly over individual upstream channels, nor in a way that accounted for downstream and upstream segment loads that account for one another.

This enhancement applies when downstream load balancing occurs on a headend system with separate upstream load balancing segments; the upstream segments are spread over multiple downstreams segments. This enhancement provides an alternative downstream load balancing scheme that accounts and makes use of per-upstream loads rather than total downstream loads.

For additional information about Load Balancing on the Cisco CMTS, refer to the following documents on Cisco.com:

- *Load Balancing and Dynamic Channel Change on the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a00801b17f2html

- *Cisco Broadband Cable Command Reference Guide*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_command_reference_book09186a0080108e88.html

## Dynamic Channel Change (DCC) for Loadbalancing

Cisco IOS Release 12.3(17a)BC introduces Dynamic Channel Change (DCC) and DCC for Load Balancing on the Cisco CMTS.

DCC in DOCSIS 1.1 dynamically changes cable modem upstream or downstream channels without forcing a cable modem to go offline, and without re-registration after the change. DCC supports four different initializations, instead of one, as in earlier DOCSIS support.

DCC and DCC for load balancing is supported on the Cisco uBR7246VXR router and the Cisco uBR10012 router with distributed cable interface line cards, including the Cisco MC28U and the Cisco MC5X20S/U/H.

- Load Balancing techniques allow for moving cable modems with DCC by using configurable initialization techniques.
- DCC allows line card channel changes across separate downstream channels in the same cable interface line card, with the DCC initialization techniques ranging from 0 to 4.
- DCC transfers cable modem state information from the originating downstream channel to the target downstream channel, and maintains synchronization of the cable modem information between the cable interface line card and the Network Processing Engine (NPE) or Route Processor (RP).
- When the target channel is in ATDMA mode, only DOCSIS 2.0-capable modems can be successfully load balanced. (Only DOCSIS 2.0-capable modems can operate on an ATDMA-only upstream channel.) Cisco recommends identical channel configurations in a load balancing group.

Dynamic Channel Change for Load Balancing entails the following new or enhanced commands in Cisco IOS Release 12.3(17a)BC, and later releases:

Global Configuration Commands

- **cable load-balance group** *group-num* **dcc-init-technique** <**0-4**>
- **cable load-balance group** *group-num* **policy { pcmm | ugs }**
- **cable load-balance group** *group-num* **threshold** {**load** | **pcmm** | **stability** | **ugs**} <**1-100**>
- **cable load-balance group** *group-num* **threshold load** <**1-100**> {**minimum**}
- **cable load-balance group** *group-num* **threshold load** <**1-100**> {**enforce**}

Testing Command

- **test cable dcc** *mac-addr* {*slot/port* | *slot/subslot/port*} *target-us-channel-id ranging-technique*

For configuration, command reference, testing, and examples for DCC on the Cisco CMTS, refer to the following documents on Cisco.com:

- *Load Balancing and Dynamic Channel Change (DCC) on the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a00801b17f2.html
- *Cisco Broadband Cable Command Reference Guide*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a00801b17f2.html

## Dynamic Ranging Support

The functionality of the **clear cable modem** <*mac-address*> **reset** command is extended to send a "Ranging Abort" message instead of just removing the SID.

A new modem state—Reset (display: resetting)— has been introduced into the modem state list. A modem is deprovisioned when moving into this state as if going offline. Move the modem to the Continue Ranging list. If a ranging request is received from the modem, send a "Ranging Abort" message. Continue until an "Initial Ranging" message is received or until normal timeout (16 attempts). If the modem does not go back to initial ranging, set it to offline.

The Reset modem state may show as follows in the output of the **show cable modem** command:

```
Cable4/0/U1 80 resetting 3575 0.25 3 0 10.30.160.26 0050.7318.e965
```

This is an intermediate state. A modem will not be in this state for more than a few seconds. If the modem does not respond, it may remain in this state for up to 30 seconds. The subsequent modem state is offline.

For additional command information about the **show cable modem** command, refer to the *Cisco Broadband Cable Command Reference Guide*.

## Enhanced Modem Status Display

The Cisco uBR7200 series universal broadband router supports polling of the CMs to obtain parameter and status information on an ongoing basis. Two new Cisco IOS commands are added to support this feature.

- The **cable modem remote** command configures the router for the polling interval; the **no** version of this command disables the status polling.

- The **show cable modem remote-query** command displays the collected information:
  - Downstream receive power level
  - Downstream signal/noise ratio (SNR)
  - Upstream power level
  - Transmit timing offset
  - Micro reflection (in dB)

For additional information about the enhanced modem status display, refer to *Modem Status Enhancements for the Cisco uBR7200 Series Cable Router* on Cisco.com.

## Entity MIB, Phase 1

For a complete list of MIBs supported by the Cisco uBR7200 series platform, refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200rn/index.htm

For descriptions of supported MIBs and how to use MIBs, refer to the *Cisco MIBs* web page on Cisco.com.

## Load Balancing for the Cisco CMTS

The Load Balancing on the Cisco CMTS feature allows service providers to optimally use both downstream and upstream bandwidth, enabling the deployment of new, high-speed services such as voice and video services. This feature also can help reduce network congestion due to the uneven distribution of cable modems across the cable network and due to different usage patterns of individual customers.

By default, the Cisco CMTS platforms use a form of load balancing that attempts to equally distribute the cable modems to different upstreams when the cable modems register. You can refine this form of load balancing by imposing a limit on the number of cable modems that can register on any particular upstream, using the cable upstream admission-control command.

However, this default form of load balancing affects the cable modems only when they initially register with the Cisco CMTS. It does not dynamically rebalance the cable modems at later times, such as when they might change upstream channels in response to RF noise problems, or when bandwidth conditions change rapidly because of real-time traffic such as Voice over IP (VoIP) and video services. It also does not affect how the cable modems are distributed among downstream channels.

For more information about the Load Balancing feature, refer to the following document on Cisco.com:

- *Configuring Load Balancing on the Cisco CMTS*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122bc/122bc_15/cmtslbg.htm

## Management Information Base (MIB) Changes and Enhancements

MIB enhancements in Cisco IOS Release 12.3(17a)BC provide enhanced management features that enable the Cisco uBR 7200 Series router and the Cisco uBR10012 router to be managed through the Simple Network Management Protocol (SNMP). These enhanced management features allow you to:

- Use SNMP set and get requests to access information in Cisco CMTS universal broadband routers.
- Reduce the amount of time and system resources required to perform functions like inventory management.
- A standards-based technology (SNMP) for monitoring faults and performance on the router.

- Support for SNMP versions (SNMPv1, SNMPv2c, and SNMPv3).
- Notification of faults, alarms, and conditions that can affect services.

### Additional Information

For a complete list of changes to the *Cisco CMTS Universal Broadband Router MIB Specifications Guide*, go to the Revision History table:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cmtsmib/cmtsmbpf.htm

To access the *Cisco CMTS Universal Broadband Router MIB Specifications Guide*, go to:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cmtsmib/index.htm

## MAX-CPE Override for Cable Modems

The following cable-specific configuration command provides a way to override the MAX-CPE parameter in the cable modem's DOCSIS configuration file:

[**no**] **cable modem max-cpe** [<*n*> | **unlimited**]

When set to unlimited or if *n* is larger than the MAX-CPE value in the configuration file of a cable modem, it overrides the configuration file value.

Note The **cable max-hosts** and **cable modem max-hosts** commands can also be used to set this value for all cable modems on a particular cable interface or for a particular cable modem.

For additional command information, refer to these documents on Cisco.com:

- *Cisco Broadband Cable Command Reference Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/
- "Maximum CPE or Host Parameters for the Cisco Cable Modem Termination System" chapter in the *Cisco Cable Modem Termination System Feature Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufg_max.htm
- *Using the max-cpe Command in the DOCSIS and CMTS*, TAC Document ID: 22177

  http://www.cisco.com/warp/public/109/max_cpe_in_docsis.html

## Per-Modem Error Counter Enhancements

The Cisco uBR7200 Series supports display of per-modem error counters with the following new command:

**show cable modem** [<*ip-addr*> | <*mac-addr*>] **error**

Below is an example display from the **show cable modem error** command:

```
Router# show cable modem error

MAC Address    SID   I/F          CRC        HCS
00d0.ba26.eee7 1     Cable4/0/U0  0          0
```

Note Both the Cyclic Redundancy Check (CRC) and Header Check Sum (HCS) are on a per- cable modem basis.

For additional command information about the **show cable modem** command, refer to the *Cisco Broadband Cable Command Reference Guide* on Cisco.com.

## Pre-equalization Control for Cable Modems

Cisco IOS Release 12.3(17a)BC introduces pre-equalization control for cable modems on a per-modem basis. This feature enhances support for pre-equalization control on an interface basis with the Organizational Unique Identifier (OUI), which is also supported.

When pre-equalization is enabled on an upstream interface, this feature allows you to disable pre-equalization adjustment selectively, for a specific cable modem or a group of cable modems. This feature prevents cable modems from flapping when processing pre-equalization requests sent from the Cisco CMTS.

### Restrictions

This feature observes the following restrictions in Cisco IOS Release 12.3(17a)BC:

- For pre-equalization to be supported on a per-modem basis, the cable modem must send verification of pre-equalization after it registers with the Cisco CMTS.
- The option of excluding the OUI is a global configuration. For the cable modem on which OUI is excluded, the excluded OUI is disabled for all interfaces. This method uses a list of OUI values, recording which modems are sent and not sent pre-equalization.
- To remove this exclusion, use the **no cable pre-equa exclude** {**modem**|**oui**} form.

### cable pre-equalization exclude

To exclude a cable modem from pre-equalization during registration with the Cisco CMTS, use the **cable pre-equalization exclude** command in global configuration mode. Exclusion is supported for a specified cable modem, or for a specified OUI value for the entire interface. To remove exclusion for the specified cable modem or interface, use the **no** form of this command. Removing this configuration returns the cable modem or interface to normal pre-equalization processes during cable modem registration.

**cable pre-equalization exclude** {**oui** | **modem**} *mac-addr*

**no cable pre-equalization exclude** {**oui** | **modem**} *mac-addr*

#### Syntax Description

| | |
|---|---|
| **oui** | Organizational Unique identifier for the interface specified. Using this keyword excludes the specified OUI during cable modem registration for the associated interface. |
| **modem** | Cable Modem identifier for the cable modem specified. Using this keyword excludes the cable modem. |
| *mac-addr* | Identifier for the OUI or cable modem to be excluded. |

#### Command Default

Pre-equalization is enabled by default on the Cisco router, and for cable modems that have a valid and operational DOCSIS configuration file. When enabled, pre-equalization sends ranging messages for the respective cable modems. When disabled with the new **exclude** command, pre-equalization is excluded for the respective cable modems.

#### Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.3(17a)BC | This command was introduced to the Cisco uBR10012 router and the Cisco uBR7246VXR router. |

## Usage Guidelines

The pre-equalization exclusion feature should be configured for the running configuration of the Network Processing Engine (NPE), the Performance Routing Engine (PRE), and the line card console.

## Examples

The following example configures pre-equalization to be excluded for the specified cable modem. Pre-equalization data is not sent for the corresponding cable modem:

```
Router(config)# cable pre-equalization exclude modem mac-addr
```

The following example configures pre-equalization to be excluded for the specified OUI value of the entire interface. Pre-equalization data is not sent for the corresponding OUI value of the entire interface:

```
Router(config)# cable pre-equalization exclude oui mac-addr
```

The following series of commands configures pre-equalization on the Cisco uBR7246VXR router with MC5X20U BPEs. On the PRE Console, configure the following commands.

```
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# cable pre-equalization exclude oui 00.09.04
Router(config)# end
Router# show run
Router# show running-config | inc oui
cable pre-equalization exclude oui 00.09.04
Router#
```

On the line card console for the same Cisco uBR7246VXR router, verify the configuration with the following command:

```
clc_7_1# show running-config | inc oui
cable pre-equalization exclude oui 00.09.04
clc_7_1#
```

The following series of commands configures pre-equalization on the Cisco uBR7246VXR router with MC28U cable interface line cards. On the Network Processing Engine (NPE) console, configure and verify with the following commands.

```
npeg1-test# conf t
Enter configuration commands, one per line. End with CNTL/Z.
npeg1-test(config)# cable pre-equalization exclude oui 00.09.24
npeg1-test(config)# end
npeg1-test#show ru
02:58:10: %SYS-5-CONFIG_I: Configured from console by consolen
npeg1-test# show running-config | inc oui
cable pre-equalization exclude oui 00.09.24
npeg1-test#
```

On the line card console for the same Cisco uBR7246VXR router, verify the configuration with the following command:

```
clc_4_0# show running-config | inc oui
cable pre-equalization exclude oui 00.09.24
clc_4_0#
```

After either of these exclusion methods for pre-equalization are configured, you can verify that all ranging messages do not include pre-equalization data. Use the following debug commands in global configuration mode:

- **debug cable range**
- **debug cable interface** cx/x/x mac-addr

Verify the ranging message for the non-excluded cable modems include pre-equalization data, and for the excluded cable modems, the ranging messages do not include such data.

The following example removes pre-equalization exclusion for the specified OUI and interface. This results in the cable modem or OUI to return to normal pre-equalization functions. Ranging messages resume sending pre-equalization data.

```
Router(config)# no cable pre-equalization exclude { oui | modem } mac-addr
```

Removal of this feature can be verified with the following **debug** command:

- **debug cable interface** cx/x/x mac-ad—Verifies the ranging message for all non-excl modems include pre-eq data, and for the excluded modems ranging messages do not include pre-eq data.

For additional information about this feature, refer to the following documents on Cisco.com:

- *DOCSIS 1.1 for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b57f.html

- *Cisco Broadband Cable Command Reference Guide*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a00801b17f2.html

## Subscriber Traffic Management (STM) Version 1.1

Cisco IOS Release 12.3(9a)BC introduces support for Subscriber Traffic Management (STM) Version 1.1 with the Cisco Broadband Troubleshooter (CBT) Version 3.2 on the Cisco uBR7246VXR universal broadband router.

STM 1.1 extends earlier STM functions to monitor a subscriber's traffic on DOCSIS 1.1 primary service flows and supports these additional features:

- Cisco Broadband Troubleshooter (CBT) 3.2 supports STM 1.1.
- DOCSIS 1.0-compliant and DOCSIS 1.1-compliant cable modem are supported.
- Monitoring and application of traffic management policies are applied on a service-flow basis.
- Monitoring window duration increased from seven to 30 days.

For additional information about STM 1.1 and Cisco CBT 3.2, refer to the following document on Cisco.com:

- *Subscriber Traffic Management for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a00801b17d0.html

- *Release Notes for Cisco Broadband Troubleshooter Release 3.2*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_command_reference_book09186a0080108e88.html

## Usage Based Billing (SAMIS)

Cisco IOS Release 12.3(9a)BC introduces the Usage-Based Billing feature on the Cisco uBR7246VXR universal broadband router, supporting DOCSIS 1.0- and DOCSIS 1.1-compliant cable modems. This feature provides subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format. SAMIS is specified by the Data-over-Cable Service Interface Specifications (DOCSIS) Operations Support System Interface (OSSI) specification.

For additional information about configuring and monitoring Usage-Based Billing (SAMIS) on the Cisco uBR7246VXR CMTS, refer to the following document on Cisco.com:

- *Usage Based Billing for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a00801ef1d7.html

# Multicast Features

The Cisco uBR7200 Series supports the following multicast options:

- Bidirectional PIM, page 1-96
- DOCSIS Set-top Gateway (DSG) 1.0, page 1-97
- Advanced-mode DOCSIS Set-Top Gateway Issue 1.1, page 1-97
- Advanced-mode DOCSIS Set-Top Gateway Issue 1.2, page 1-99
- IGMP Version 3, page 1-99
- IP Multicast Load Splitting across Equal-Cost Paths, page 1-99
- IP Multicast over ATM Point-to-Multipoint Virtual Circuits, page 1-100
- IP Multicast over Token Ring LANs, page 1-100
- Source Specific Multicast, page 1-101
- Stub IP Multicast Routing, page 1-101

## Bidirectional PIM

**Cisco IOS Releases**—Supported in the Cisco IOS 12.2 BC and 12.1 EC release trains.

Bidirectional Protocol Independent Multicast (bidir-PIM) is a variant of the Protocol Independent Multicast (PIM) suite of routing protocols for IP multicast. In PIM, packet traffic for a multicast group is routed according to the rules of the mode configured for that multicast group. The Cisco IOS implementation of PIM supports three modes for a multicast group:

- Bidirectional mode
- Dense mode
- Sparse mode

A router can simultaneously support all three modes or any combination of them for different multicast groups. In bidirectional mode, traffic is only routed along a bidirectional shared tree that is rooted at the rendezvous point (RP) for the group. In bidir-PIM, the IP address of the RP acts as the key to having all routers establish a loop-free spanning tree topology rooted in that IP address. This IP address does not need to be a router, but can be any unassigned IP address on a network that is reachable throughout the PIM domain. Using this technique is the preferred configuration for establishing a redundant RP configuration for bidir-PIM.

For additional information about bidir-PIM and its configuration, refer to *Configuring Bidirectional PIM* in the *Cisco IOS IP Configuration Guide*, Release 12.2 on Cisco.com.

## DOCSIS Set-top Gateway (DSG) 1.0

The following DSG 1.0 features were added for multiple Cisco CMTS platforms in Cisco IOS release 12.3(9a)BC:

- Vendor names are supported to 20 characters per SNMP requirements (all platforms).
- SNMP MIB support introduced for the DSG-IF-MIB.
- Multicast MAC addresses are supported for DSG tunnels. DSG tunnel MAC addresses are no longer limited only to unicast addresses.
- DSG 1.0 prevents the configuration of any reserved or otherwise inappropriate IP multicast addresses.

For additional information about configuring and using DSG 1.0 on the Cisco uBR7246VXR router, refer to the following document on Cisco.com:

- *DOCSIS Set-Top Gateway for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a00802065c8.html

## Advanced-mode DOCSIS Set-Top Gateway Issue 1.1

Cisco IOS Release 12.3(13a)BC introduces support for DOCSIS Set-Top Gateway (DSG) Issue 1.1 on the Cisco uBR10012 router. DOCSIS Set-Top Gateway (DSG) 1.1 introduces Advanced mode DSG functionality based on Cablelabs specification CM-SP-DSG-I03-041124 on the Cisco uBR7246VXR and uBR10012 platforms.

DSG 1.1 introduces support for several DOCSIS 1.1 networks and their multiple service operators (MSOs):

- Supports advanced mode capabilities such as DCD, Regionalization, Fragmentation, and Quality of Service (QoS).
- Retains the essential nature of out of band (OOB) messaging, but moves it to a modern technology base, offering enhanced security for Multicast delivery of OOB messages dynamically to Set-top boxes.
- Replaces single-vendor, low-density, special-purpose equipment on the network, with significantly increased subscriber bandwidth and traffic.
- Consolidates cable modem and STB data traffic on a shared DOCSIS channel.
- Increases high-speed data (HSD) services to cable TV subscribers over the DOCSIS 1.1 infrastructure,
- Extends support for DOCSIS 1.1 digital video broadcast traffic.
- Enables shared or dedicated support for either HSD or video traffic.
- Supports one- or two-way operations, and advanced, two-way interactive applications such as streaming video, Web browsing, email, real-time chat applications, and targeted advertising services.

These powerful advantages maximize the performance and return of hybrid fiber-coaxial (HFC) plant investments.

## Changes from Cisco DSG 1.0

DSG Issue 1.0 is oriented to the DOCSIS DSG-I01 specifications, while DSG Issue 1.1 is oriented towards DOCSIS DSG-I02 specifications, to include the new Advanced Mode DSG (A-DSG).

The following DSG 1.1 features are supported in 12.3(13a)BC while continuing support for Basic Mode DSG:

- DSG 1.1 enables the learning of dynamic tunnel definitions. DSG 1.0 only had static tunnel definitions (programmed into the set-top box).
- DSG 1.1 features new Cisco IOS command-line interface (CLI) configuration and **show** commands for A-DSG configuration and network information.

Unlike earlier issues of DSG, Advanced-mode DSG (A-DSG) uses a DOCSIS MAC Management Message called the Downstream Channel Descriptor (DCD) message, and this DCD message manages the DSG Tunnel traffic. The DCD message is sent once per second on each downstream and is used by the DSG Client to determine which tunnel and classifier to use.

The DCD has a DSG address table located in the DOCSIS MAC management message. The primary difference between DSG 1.0 (and earlier issues) and A-DSG 1.1 is that advanced mode uses DCD messages to manage the DSG tunnels.

The DCD message contains a group of DSG Rules and DSG Classifiers, including the following:

- DSG rules and rule priority
- DSG classifiers
- DSG channel list type/length value (TLV)
- DSG client identifier (whether broadcast, CA System, application, or MAC-level)
- DSG timer list
- DSG upstream channel ID (UCID) list
- Vendor-specific information field

## Prerequisites for DSG 1.1

- Cisco IOS release 12.3(13a)BC or a later 12.3 BC release are required.
- Cisco DSG 1.1 is supported on the Cisco uBR10012 router with PRE2 performance routing engine modules.
- Cisco DSG 1.1 is supported on the Cisco uBR10012 router with the following cable interface line cards and broadband processing engines (BPEs):
  - Cisco uBR10-LCP2-MC16C/MC16E/MC16S Cable Interface Line Card
  - Cisco uBR10-LCP2-MC28C Cable Interface Line Card
  - Cisco uBR10-MC5X20S/U Broadband Processing Engine

## Restrictions and Caveats for DSG 1.1

Cisco DSG 1.1 has the following restrictions:

- Cisco DSG 1.1 does not support the PRE1 module on the Cisco uBR10012 router.
- Cisco DSG 1.1 does not support Service Flow Quality of Service (QoS), which is available at Layer 3.
- Cisco DSG 1.1 does not support tunnel security, but strictly access control lists (ACLs).
- Cisco DSG 1.1 does not support subinterfaces.
- Cisco DSG 1.1 does not support HCCP N+1 interoperability.
- Cisco DSG 1.1 does not support SNMP MIBS for A-DSG.

### Additional Information about DSG 1.1

- *Advanced-mode DOCSIS Set-Top Gateway Issue 1.1 for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guides_list.html
- *DOCSIS Set-Top Gateway (DSG) for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a00802065c8.html
- *Cisco DOCSIS Set-top Gateway* White Paper

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_white_paper09186a00801b3f0f.shtml
- CableLabs *DOCSIS Set-top Gateway (DSG) Interface Specification SP-DSG-I03-041124*

  http://www.cablemodem.com/downloads/specs/CM-SP-DSG-I03-041124.pdf

## Advanced-mode DOCSIS Set-Top Gateway Issue 1.2

Cisco IOS Release 12.3(17a)BC2 introduces support for advanced-mode DOCSIS Set-Top Gateway (DSG) Issue 1.2. DSG Issue 1.2 introduces support for the latest DOCSIS Set-Top specification from CableLabs™:

- *DOCSIS Set-top Gateway (DSG) Interface Specification*, CM-SP-DSG-I05-050812

  http://www.cablelabs.com/specifications/archives/CM-SP-DSG-I05-050812-Superseded.pdf

Advanced-mode DSG 1.2 is a powerful tool in support of latest industry innovations. Advanced-mode DSG 1.2 offers substantial support for enhanced DOCSIS implementation in the Broadband Cable environment. The set-top box dynamically learns the overall environment from the Cisco Cable Modem Termination System (CMTS), to include MAC address, traffic management rules, and classifiers. For additional information, refer to the following document on Cisco.com:

- *Advanced-mode DOCSIS Set-Top Gateway 1.2 for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guides_list.html

## IGMP Version 3

Internet Group Management Protocol (IGMP) is a protocol used by IPv4 systems to report IP multicast group memberships to neighboring multicast routers. On networks with hosts directly attached, IGMP Version 3 (IGMPv3) adds support for “source filtering”, which enables a multicast receiver to signal to a router which groups it wants to receive multicast traffic from, and from which source(s) this traffic is expected. Based on this membership information, Cisco IOS software only forwards traffic that is requested by the host or by other routers via Protocol Independent Multicast [PIM]) to that network. In addition to restricting traffic on the network of the receiver host, IGMPv3 membership information can also be propagated to multicast routing protocols to enable the forwarding of traffic from permitted sources or to restrict traffic from denied sources along the entire multicast data delivery path.

In the Source Specific Multicast (SSM) feature, introduced in Cisco IOS Release 12.1(3)T, hosts must explicitly include sources when joining a multicast group (this is known as “channel subscription”). IGMPv3 is the industry-designated standard protocol for hosts to signal channel subscriptions in SSM. In deployment cases where IGMPv3 cannot be used (for example, if it is not supported by the receiver host or its applications), there are two other mechanisms to enable SSM: URL Rendezvous Directory (URD) and IGMP Version 3 lite (IGMP v3lite). Both of these features were introduced with SSM in Cisco IOS Release 12.1(3)T.

## IP Multicast Load Splitting across Equal-Cost Paths

You can now configure load splitting of IP multicast traffic across equal-cost paths. Prior to this feature, when there were equal-cost paths between routers, IP multicast packets traversed only one path. If a tunnel was configured, the same next hop was always used, and no load splitting occurred. IP multicast

load splitting is accomplished indirectly by consolidating the available bandwidth of all the physical links into a single tunnel interface. The underlying physical connections then use existing unicast load-splitting mechanisms for the tunnel (multicast) traffic.

Note This feature is load splitting the traffic, not load balancing the traffic.

By configuring load splitting among equal-cost paths, you can use your links between routers more efficiently when sending IP multicast traffic. For configuration information, refer to the following document on Cisco.com:

- *"Configuring IP Multicast Routing"* chapter in the *Cisco IOS IP Configuration Guide*, Release 12.2 guide on Cisco.com:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt3/

## IP Multicast over ATM Point-to-Multipoint Virtual Circuits

IP multicast over ATM point-to-multipoint virtual circuits is a feature that dynamically creates ATM point-to-multipoint SVCs to handle IP multicast traffic more efficiently.

The feature can enhance router performance and link utilization because packets are not replicated and sent multiple times over the ATM interface.

For configuration information, refer to the following document on Cisco.com:

- *"Configuring IP Multicast Routing"* chapter in the *Cisco IOS IP Configuration Guide*, Release 12.2 guide on Cisco.com:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt3/

## IP Multicast over Token Ring LANs

By default, IP multicast datagrams on Token Ring LAN segments use the MAC-level broadcast address 0xFFFF.FFFF.FFFF. That default places an unnecessary burden on all devices that do not participate in IP multicast. The IP multicast over Token Ring LANs feature defines a way to map IP multicast addresses to a single Token Ring MAC address.

This feature defines the Token Ring functional address (0xc000.0004.0000) that should be used over Token Ring. A functional address is a severely restricted form of multicast addressing implemented on Token Ring interfaces. Only 31 functional addresses are available. A bit in the destination MAC address designates it as a functional address.

The implementation used by Cisco complies with RFC 1469, *IP Multicast over Token-Ring Local Area Networks*.

If you configure this feature, IP multicast transmissions over Token Ring interfaces are more efficient than they formerly were. This feature reduces the load on other machines that do not participate in IP multicast because they do not process these packets.

For configuration information, refer to the following document on Cisco.com:

- *"Configuring IP Multicast Routing"* chapter in the *Cisco IOS IP Configuration Guide*, Release 12.2 guide on Cisco.com:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt3/

## Source Specific Multicast

The Source Specific Multicast (SSM) feature is an extension of IP multicast, where datagram traffic is forwarded to receivers from only those multicast sources that the receivers have explicitly joined. When SSM is used, only source-specific multicast distribution trees (no shared trees) are created.

SSM is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is the core networking technology for the Cisco implementation of the IP Multicast lite suite of solutions targeted for audio and video broadcast application environments.

This feature module introduces the following Cisco IOS components that support SSM:

- PIM-SS (PIM source specific)
- Internet Group Management Protocol Version 3 lite (IGMP v3lite)
- URL Rendezvous Directory (URD)

The Cisco implementation of SSM will soon be deployed with Internet Group Management Protocol Version 3 (IGMPv3) support. Cisco developed IGMP v3lite and URD to support the deployment of applications using SSM services before the introduction of IGMPv3.

## Stub IP Multicast Routing

When you use PIM in a large network, there are often stub regions over which the administrator has limited control. To reduce the configuration and administration burden, you can configure a subset of PIM functionality that provides the stub region with connectivity, but does not allow it to participate in or potentially complicate any routing decisions.

Stub IP multicast routing allows simple multicast connectivity and configuration at stub networks. It eliminates periodic flood-and-prune behavior across slow-speed links (ISDN and below) using dense mode. It eliminates that behavior by using forwarded IGMP reports as a type of Join message and using selective PIM message filtering.

Stub IP multicast routing allows stub sites to be configured quickly and easily for basic multicast connectivity, without the flooding of multicast packets and subsequent group pruning that occurs in dense mode, and without excessive administrative burden at the central site.

For configuration information, refer to the following document on Cisco.com:

- *"Configuring IP Multicast Routing"* chapter in the *Cisco IOS IP Configuration Guide*, Release 12.2 guide on Cisco.com:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt3/

# PacketCable and Voice Support Features

The Cisco uBR7200 Series supports the following PacketCable and PacketCable MultiMedia feature:

- PacketCable 1.0 With CALEA, page 1-102

## PacketCable 1.0 With CALEA

Cisco IOS Release 12.3(9a)BC introduces DOCSIS 1.1 support for PacketCable 1.0 with Communications Assistance for Law Enforcement Act (CALEA) on the Cisco uBR10012 universal broadband router with the Cisco uBR10-MC5X20S/U Broadband Processing Engine (BPE).

PacketCable is a program initiative from Cablelabs and its associated vendors to establish a standard way of providing packet-based, real-time video and other multimedia traffic over hybrid fiber-coaxial (HFC) cable networks. The PacketCable specification is built upon the Data-over-Cable System Interface Specifications (DOCSIS) 1.1, but it extends the DOCSIS protocol with several other protocols for use over non-cable networks, such as the Internet and the public switched telephone network (PSTN).

This allows PacketCable to be an end-to-end solution for traffic that originates or terminates on a cable network, simplifying the task of providing multimedia services over an infrastructure composed of disparate networks and media types. It also provides an integrated approach to end-to-end call signaling, provisioning, quality of service (QoS), security, billing, and network management.

Cisco IOS Release 12.2(11)BC1 and later releases in the Cisco IOS 12.3 release train support the PacketCable 1.0 specifications and the CALEA intercept capabilities of the PacketCable 1.1 specifications.

For additional information about configuring PacketCable on the Cisco CMTS, refer to the following document on Cisco.com:

- *Configuring PacketCable on the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b576.html

# Security Features

The Cisco uBR7200 Series supports multiple security features:


- Access Control Lists, page 1-103
- Automated Double Authentication, page 1-103
- Cable Modem and Multicast Authentication Using RADIUS, page 1-103
- Cable Source Verification (cable source-verify Command), page 1-104
- Cisco IOS Firewall Feature Set, page 1-104
- Cisco IOS Firewall Feature Enhancements, page 1-104
- Dynamic Mobile Hosts, page 1-105
- Dynamic Shared Secret for DOCSIS, page 1-105
- Dynamic Shared Secret (DMIC) with OUI Exclusion for DOCSIS, page 1-106
- HTTP Security, page 1-106
- Named Method Lists for AAA Authorization & Accounting, page 1-107
- Per-Modem Filters (Per-Modem and Per-Host Access Lists), page 1-107
- Per-User Configuration, page 1-107
- Redirect-Number Support for RADIUS and TACACS+ Servers, page 1-107
- Reflexive Access Lists, page 1-108
- Secure Shell (SSH) Supported in "k1" Images for Cisco uBR7200, page 1-108

- Turbo Access Control Lists, page 1-108
- Vendor-Proprietary RADIUS Attributes, page 1-109

For additional BPI information and configuration steps, refer to the *DOCSIS 1.1 for the Cisco uBR7200 Series Universal Broadband Routers* feature module on Cisco.com, and to additional documents cited below:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200sw/index.htm

## Access Control Lists

Access control lists (ACLs) are supported on the Cisco uBR7200 Series in Cisco IOS Release 12.2(4)XF1 and later XF and BC releases, and in 12.2(10)EC and later EC releases.

The Cisco uBR7200 Series provides basic traffic filtering capabilities with access control lists (ACLs — also referred to as access lists). Access lists can be configured for all routed network protocols (IP, AppleTalk, and so on) to filter the packets of those protocols as the packets pass through a router.

You can configure access lists at your router to control access to a network: access lists can prevent certain traffic from entering or exiting a network.

For complete information about access lists, see the *Traffic Filtering and Firewall* volume in the *Cisco IOS Release 12.1 Security Configuration Guide*, available on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt3/index.htm

The Cisco uBR7200 Series also supports SNMP access lists and Turbo Access Control Lists, and these are described elsewhere in this chapter.

## Automated Double Authentication

The automated double authentication feature enhances the existing double authentication feature. Previously, with the existing double authentication feature, a second level of user authentication is achieved when the user accesses the network access server or router through Telnet and enters a user name and password. Now, with automated double authentication, the user does not have to Telnet anywhere but instead responds to a dialog box that requests a user name and password or PIN.

For information about the existing double authentication feature, refer to the following document on Cisco.com:

- "Configuring Authentication" chapter of the *Cisco IOS Security Configuration Guide*, Release 12.2

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/

## Cable Modem and Multicast Authentication Using RADIUS

As an enhancement to Baseline Privacy, the Cisco uBR7200 series universal broadband routers can be configured for cable modem and multicast authentication using the Remote Authentication Dial-In User Server (RADIUS) protocol, an access server authentication, authorization, and accounting protocol originally developed by Livingston, Inc. This release also supports additional vendor-proprietary RADIUS attributes.

When a cable modem comes online or when a JOIN request is sent through a multicast data stream, the Cisco uBR7200 series universal broadband routers send relevant information to RADIUS servers for cable modem/host authentication. This feature can be configured on a per-interface basis.

An Internet Engineering Task Force (IETF) draft standard, RFC 2138, defines the RADIUS protocol. RFC 2139 defines the corresponding RADIUS accounting protocol. Additional RFC drafts define vendor-proprietary attributes and MIBs that can be used with an SNMP manager.

For additional information, refer to the following document on Cisco.com:

- "Security Server Protocols" chapters of the *Cisco IOS Security Configuration Guide*, Release 12.2

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsecsp/index.htm

## Cable Source Verification (cable source-verify Command)

The **cable source-verify** command helps to prevent the spoofing of IP addresses by CMs or their CPE devices by verifying that the upstream packets coming from each cable modem are known to be associated with the IP address in that packet. Packets with IP addresses that do not match those associated with the cable modem are dropped.

Note The **cable source-verify** [**dhcp**] cable interface command specifies that DHCP lease-query requests are sent to verify any unknown source IP address found in upstream data packets. This feature requires a DHCP server that supports the new LEASEQUERY message type.

For additional information about the **cable source-verify** command, refer to the *Cisco Broadband Cable Command Reference Guide* on Cisco.com.

## Cisco IOS Firewall Feature Set

The Cisco IOS Firewall feature set interoperates in seamless fashion with Cisco IOS software, providing great value for the many benefits it delivers. The most outstanding benefits include:

- Flexibility — installed on a Cisco router, this all-in-one scalable solution performs multiprotocol routing, perimeter security, intrusion detection, VPN functionality, and per-user authentication and authorization.
- Investment protection — integrating firewall functionality into a multiprotocol router leverages an existing router investment without the cost and learning curve associated with a new platform.
- VPN support — deploying Cisco IOS Firewall with Cisco IOS encryption and QoS VPN features enables extremely secure, low-cost transmissions over public networks and ensures mission—critical application traffic receives high priority delivery.
- Scalable deployment — available for a wide variety of router platforms, the Cisco IOS Firewall scales to meet any network`s bandwidth and performance requirements.
- Easier management — with Cisco ConfigMaker software, a network administrator can configure Cisco IOS security features (including the Cisco IOS Firewall, Network Address Translation, and Cisco IPSec) from a central console over the network.

For additional Cisco IOS firewall information, refer to the document titled *Cisco IOS Firewall Feature Set* on Cisco.com.

## Cisco IOS Firewall Feature Enhancements

Cisco IOS Release 12.1(1a)T1 enhances the previous Cisco IOS Secure Integrated Software feature set with the following set of features:

- Context-Based Access Control (CBAC) that intelligently filters TCP and UDP packets based on the application-layer protocol. This includes Java applets, which can be blocked completely or allowed only from known and trusted sources.
- Detection and prevention of the most common denial of service (DoS) attacks, such as ICMP and UDP echo packet flooding, synchronize/start (SYN) packet flooding, half-open or other unusual TCP connections, and deliberate misfragmentation of IP packets.
- Support for a broad range of commonly used protocols, including H.323 and NetMeeting, FTP, HTTP, MS Netshow, RPC, SMTP, SQL*Net, and TFTP.
- Authentication Proxy for authentication and authorization of web clients on a per-user basis.

- Dynamic port mapping that maps the default port numbers for well-known applications to other port numbers. This can be done on a host-by-host basis or for an entire subnet, providing a large degree of control over which users can access different applications.
- Configurable alerts and audit trail.
- Intrusion Detection System (IDS) that recognizes the signatures of 59 common attack profiles. When an intrusion is detected, IDS can either send an alarm to a syslog server or to NetRanger Director, drop the packet, or reset the TCP connection.
- User-configurable audit rules.
- Configurable real-time alerts and audit trail logs.

For general information, see the description of the Cisco IOS Firewall Feature Set in the Cisco Product Catalog. For detailed information, refer to these documents on Cisco.com:

- *Cisco IOS Firewall Feature Set* documentation
- In particular, refer to the "Security Configuration Guide, "Traffic Filtering" chapter:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/

## Dynamic Mobile Hosts

This feature addresses a security hole that occurs when the Cisco uBR7200 series router supports mobile hosts. (Mobile host are hosts that can move from one modem to another modem.) Anyone who knows the MAC address of a mobile host can "fake" the mobile host, thereby causing denial of access for the real mobile host.

To avoid this security hole, the Dynamic Mobile Hosts feature pings the mobile host on the old service identifier (SID) to verify that the host has indeed been moved.

A DHCP server is used to verify addresses and can be configured with the **cable source-verify dhcp** command; the **no cable arp** command should be configured in the CMTS to prevent it from sending ARP requests.

For additional information, refer to the *Cisco Broadband Cable Command Reference Guid*e on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm

## Dynamic Shared Secret for DOCSIS

The Dynamic Shared Secret feature provides service providers a way of providing higher levels of security for their Data-over-Cable Service Interface Specifications (DOCSIS) cable networks, by using randomized, single-use shared secrets to verify the DOCSIS configuration files that are downloaded to each cable modem. The Dynamic Shared Secret feature is enabled using the **cable dynamic-secret** interface configuration command.

The Dynamic Shared Secret feature automatically creates a unique DOCSIS shared secret on a per-modem basis, creating a one-time use DOCSIS configuration file that is valid only for the current session. This ensures that a DOCSIS configuration file that has been downloaded for one cable modem can never be used by any other modem, nor can the same modem reuse this configuration file at a later time.

This patent-pending feature is designed to guarantee that all registered modems are using only the quality of service (QoS) parameters that have been specified by the DOCSIS provisioning system for that particular modem at the time of its registration.

For additional information, refer to the following document on Cisco.com:

- *Configuring a Dynamic Shared Secret for the Cisco CMTS* document:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122bc/122bc_15/ubrdmic.htm

Note The Dynamic Shared Secret feature does not affect the use of the original shared secret or secondary shared secrets that are configured using the **cable shared-secondary-secret** and **cable shared-secret** commands. If these shared secrets are configured, the Cisco CMTS continues to use them to validate the original DOCSIS configuration file that is downloaded from the TFTP server. If the DOCSIS configuration file fails to pass the original or secondary shared secret verification checks, the cable modem is not allowed to register, and the Dynamic Shared Secret feature is not invoked for that particular cable modem.

Tip Verify that a cable modem is able to register with the Cisco CMTS before enabling the Dynamic Shared Secret feature.

## Dynamic Shared Secret (DMIC) with OUI Exclusion for DOCSIS

Cisco IOS Release 12.3(9a)BC introduces the option of *excluding* the Organizational Unique Identifiers (OUIs) from being subjected to the DMIC check. The new **cable dynamic-secret exclude** command allow specific cable modems to be excluded from the Dynamic Shared Secret feature on the following Cisco CMTS platforms:

- Cisco uBR7246VXR universal broadband router
- Cisco uBR10012 universal broadband router

The Dynamic Shared Secret feature automatically creates a unique DOCSIS shared secret on a per-modem basis, creating a one-time use DOCSIS configuration file that is valid only for the current session. This ensures that a DOCSIS configuration file that has been downloaded for one cable modem can never be used by any other modem, nor can the same modem reuse this configuration file at a later time.

This patent-pending feature is designed to guarantee that all registered modems are using only the quality of service (QoS) parameters that have been specified by the DOCSIS provisioning system for that particular modem at the time of its registration.

For additional command information, refer to the following document on Cisco.com:

- *Configuring a Dynamic Shared Secret for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a00801b17cc.html

- *Cisco Broadband Cable Command Reference Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm

## HTTP Security

Cisco IOS Release 12.2(4)BC1 includes the HTTP security solution introduced for earlier Cisco IOS releases and router platforms. For additional information, refer to the document titled *Cisco IOS HTTP Server Query Vulnerability*, Revision 1.3 on Cisco.com:

http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml

## Named Method Lists for AAA Authorization & Accounting

Named method lists for Authentication, Authorization, and Accounting (AAA) allow you to define different methods for authorization and accounting and apply those methods on a per-interface or per-line basis. For additional information, refer to the following document on Cisco.com:

- *Configuring Authorization*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathor.htm

## Per-Modem Filters (Per-Modem and Per-Host Access Lists)

Per-modem filters provide you with the ability to filter incoming packets from individual hosts or cable interfaces based on the source Media Access Controller (MAC) or Internet Protocol (IP) address. This allows access lists to be specified on a per-interface and per-direction basis. The packets received from cable interfaces and/or individual hosts are filtered based on the cable interface or the host from which the packets are received.

For additional information, refer to these documents on Cisco.com:

- "Configuring Per-Modem Filters" section on page 5-8
- *Cisco Broadband Cable Command Reference Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm

## Per-User Configuration

Per-user configuration provides a flexible, scalable, easily maintained solution for customers with a large number of dial-in users. This solution can tie together the following dial-in features:

Virtual template interfaces, generic interface configuration and router-specific configuration information stored in the form of a virtual template interface that can be applied (cloned) to a virtual access interface each time any user dials in. This is described in the following document on Cisco.com:

- "Virtual Templates, Profiles, and Networks" chapter in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fdial_c/

AAA per-user security and interface configuration information stored on a separate AAA server and sent by the AAA server to the access server or router in response to authorization requests during the PPP authentication phase. The per-user configuration information can add to or override the generic configuration on a virtual interface.

Virtual profiles, which can use either or both of the two sources of information above for virtual interface configuration. When a user dials in, virtual profiles can apply the generic interface configuration and then apply the per-user configuration to create a unique virtual access interface for that user.

A virtual access interface created dynamically for any user dial-in session is deleted when the session ends. The resources used during the session are returned for other dial-in uses.

This set of features is supported on all platforms that support Multilink PPP.

## Redirect-Number Support for RADIUS and TACACS+ Servers

The telco-return RADIUS server has been enhanced to provide additional authentication information, allowing an administrator to determine whether a subscriber dialed a number that requires special billing arrangements (such as a toll-free number). If a telco return customer is being authenticated by a TACACS+ or RADIUS server, and if the number dialed by the cable modem is being redirected to another number for authentication, the system can include the original number in the information sent to the authentication server. The original number can be sent as a Cisco vendor-specific attribute (VSA) for TACACS+ servers and as RADIUS Attribute 93 (Ascend-Redirect-Number) for RADIUS servers.

For additional information, refer to the following document on Cisco.com:

- "Telco Return for the Cisco Cable Modem Termination System" chapter in the *Cisco Cable Modem Termination System Feature Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufg_telc.htm

## Reflexive Access Lists

Reflexive access lists allow IP packets to be filtered based on upper-layer session information. You can use reflexive access lists to permit IP traffic for sessions originating from within your network but to deny IP traffic for sessions originating from outside your network. This is accomplished by reflexive filtering, a kind of session filtering.

Reflexive access lists can be defined with extended named IP access lists only. You cannot define reflexive access lists with numbered or standard named IP access lists or with other protocol access lists.You can use reflexive access lists in conjunction with other standard access lists and static extended access lists.

Reflexive access lists are an important part of securing your network against network hackers, and can be included in a firewall defense. Reflexive access lists provide a level of security against spoofing and certain denial-of-service attacks. Reflexive access lists are simple to use, and, compared to basic access lists, provide greater control over which packets enter your network.

For additional information, refer to the following document on Cisco.com:

- *Configuring IP Session Filtering (Reflexive Access Lists)*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt3/

## Secure Shell (SSH) Supported in "k1" Images for Cisco uBR7200

In Cisco IOS Release 12.1 T, the definition of "k1" images for Cisco uBR924 cable access routers was changed from support for BPI only, to also include support for Secure Shell (SSH). This change caused an inconsistency with Cisco uBR7200 series images, since the definition of "k1" for the Cisco uBR7200 was not changed and did not include SSH.

Cisco uBR7200 series universal broadband routers support the Cisco IOS Firewall feature. This feature set offers Network Address Translation (NAT) and is designed to prevent unauthorized, external access to your internal network, blocking attacks on your network, while still allowing authorized users to access network resources. This feature is described in detail in the *Cisco IOS Firewall* web page on Cisco.com.

## Turbo Access Control Lists

The Turbo Access Control List (ACL) feature processes access lists more expediently, providing faster functionality for routers equipped with the feature. ACLs are normally searched sequentially to find a matching rule, and ACLs are ordered specifically to take this factor into account. Because of the increasing needs and requirements for security filtering and packet classification, ACLs can expand to the point that searching the ACL adds a significant amount of time and memory when packets are being forwarded. Moreover, the time taken by the router to search the list is not always consistent, adding a variable latency to the packet forwarding. A high CPU load is necessary for searching an ACL with several entries.

The Turbo ACL feature compiles the ACLs into a set of lookup tables, while maintaining the first match requirements. Packet headers are used to access these tables in a small, fixed number of lookups, independently of the existing number of ACL entries. The benefits of this feature include:

- For ACLs larger than 3 entries, the CPU load required to match the packet to the pre-determined packet-matching rule is lessened. The CPU load is fixed, regardless of the size of the ACL, allowing for larger ACLs without incurring any CPU overhead penalties. The larger the ACL, the greater the benefit.

- The time taken to match the packet is fixed, so that latency of the packets are smaller (significantly in the case of large ACLs) and more importantly, consistent, allowing better network stability and more accurate transit times.

For additional feature and configuration information, refer to the following document on Cisco.com:

- "Enabling Turbo Access Control Lists" topic of the "IP Addressing and Services" section of the *Cisco IOS IP Configuration Guide*, Release 12.2

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfip.htm#xtocid17

## Vendor-Proprietary RADIUS Attributes

Remote Authentication Dial-In User Service (RADIUS) attributes are used to define specific authentication, authorization, and accounting elements in a user profile, which is stored on the RADIUS daemon. Cisco supports a variety of vendor-proprietary RADIUS attributes. For additional information, refer to the appendix "Radius Attributes" in the *Cisco IOS Security Configuration Guide*, Release 12.2 on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fappendx/fradattr/

# SNMP Features and Enhancements

Multiple Cisco IOS releases that support the Cisco uBR7200 Series include enhanced Simple Network Management Protocol (SNMP) features:

- Individual SNMP Trap Support, page 1-109
- LinkUp/Down Traps Support (RFC 2233), page 1-110
- SNMPv2C, page 1-110
- SNMPv3, page 1-111
- SNMP Cable Modem Remote Query, page 1-111
- SNMP Management Information Base (MIB) Enhancements, page 1-111
- SNMP MIBs Changes and Updates in Cisco IOS Release 12.3(9a)BC, page 1-117
- SNMP Warm Start Trap, page 1-119

## Individual SNMP Trap Support

The Individual SNMP Trap Support feature adds the ability to enable or disable SNMP system management notifications (traps) individually. SNMP traps that can be specified are "authentication", "linkup", "linkdown", and "coldstart." This feature expands the functionality of the **snmp-server enable traps** command.

Note When the **snmp-server enable traps** command is given without any options, it enables all traps, which can generate a significant number of traps at key events, such as system power-up. If the SNMP queue is not large enough to handle all of the traps, new traps will be dropped without notification until the existing traps are sent and slots become available in the queue.

You can do two things to avoid dropping traps in this situation:

- Increase the SNMP trap queue size. The default queue size is 10, which is insufficient to handle all traps. Use the snmp-server queue-length length global configuration command to increase the queue size. The length parameter can range from 10 to 1000. Increase the queue size until traps are no longer dropped.
- Disable unneeded SNMP traps. For example, if you do not need SYSLOG traps (which are sent for every message displayed on the console), disable those traps as follows:

```
Router(config)# snmp-server enable traps
Router(config)# no snmp-server enable traps syslog
```

For additional feature information, refer to the following document on Cisco.com:

- *Individual SNMP Trap Support*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtitraps.htm

## LinkUp/Down Traps Support (RFC 2233)

The objects in the varbind list, based on the Internet Engineering Task Force (IETF) standard, are defined in IF-MIB. Since IF-MIB supports subinterfaces, all objects in this varbind list are also supported for subinterfaces. The feature allows you to base the Link Up/Down trap varbind list on a Cisco-specific or IETF standard with a new CLI configuration command.

To enable linkUp/linkDown Simple Network Management Protocol (SNMP) traps which are compliant with RFC2233, use the **snmp-server trap link** command in global configuration mode. To disable IETF compliant functionality and revert to the default Cisco implementation of linkUp/linkDown traps, use the **no** form of this command.

**snmp-server link-trap [cisco | ietf]**

**no snmp-server link-trap [cisco | ietf]**

Syntax Description

| | |
|---|---|
| **cisco** | The default is a Cisco-specific link trap (**snmp-server link-trap cisco**). The user can switch between Cisco and IETF standard. |
| **ietf** | This keyword links functionality of SNMP linkUp/linkDown traps to the Internet Engineering Task Force (IETF) standard (as opposed to the previous Cisco implementation). |

## SNMPv2C

SNMPv2 defines several new macros. The following macros identify a MIB as an SNMPv2 MIB:

- MODULE-IDENTITY
- MODULE-COMPLIANCE
- OBJECT-GROUP
- NOTIFICATION-TYPE TEXTUAL-CONVENTION

For additional information about SNMPv2C, refer to the document titled *Simple Network Management Protocol (SNMP) Technical Tips* on Cisco.com.

## SNMPv3

SNMPv3 is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security features provided in SNMPv3 are:

- Message integrity—Ensures that a packet has not been tampered with in-transit.
- Authentication—Determines the message is from a valid source.
- Encryption—Scrambling the contents of a packet prevents it from being seen by an unauthorized source.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine which security mechanism is employed when handling an SNMP packet.

For additional information about SNMPv3, refer to the document titled *SNMPv3* feature summary on Cisco.com.

## SNMP Cable Modem Remote Query

### Configuring Remote Modem Monitoring

To specify how often SNMP polls the modem, and to configure access, use the **cable modem remote-query** command in global configuration mode. To disable the gathering of cable modem statistics, use the **no** form of this command.

**cable modem remote-query** *polling-interval community-string*

**no cable modem remote-query**

Syntax Description

| | |
|---|---|
| *polling-interval* | Specifies how often the CMTS polls for cable modem statistics. Valid range is from 1 to 86,400 seconds. |
| *community-string* | Defines the Simple Network Management Protocol (SNMP) community string. |

### Verifying Remote Query Information

To display information from a queried modem, enter the **show cable modem remote-query** command in global configuration mode.

### Troubleshooting Tips

To display debugging information, use the **debug cable remote-query** command in global configuration mode.

For additional configuration and feature information, refer to *Modem Status Enhancements for the Cisco uBR7200 Series Cable Router* on Cisco.com.

## SNMP Management Information Base (MIB) Enhancements

### Obtaining Current Management Information Bases

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, refer to the *Cisco MIB* web page on Cisco.com. For additional information, refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200rn/index.htm

## Categories of Supported Management Information Bases

The Cisco uBR7200 series universal broadband routers support the following categories of MIBs:

- SNMP standard MIBs—These MIBs are required by any agent supporting SNMPv1 or SNMPv2 network management.
- Cisco's platform and network-layer enterprise MIBs—Common across most of Cisco's router platforms. If your network management applications are already configured to support other Cisco routers, such as the 2600 series or 7200 series, no further configuration is needed unless the version of Cisco IOS software being used has updated these MIBs.
- Cable-specific MIBs—Provide information about the cable interfaces and related information on the uBR7200 series routers. They include both DOCSIS-specific MIBs and Cisco-specific enterprise MIBs. If your network management applications have not already been configured for the uBR7200 series routers, these MIBs must be loaded.
- Deprecated MIBs—Supported in earlier releases of Cisco IOS software but have been replaced by more standardized, scalable MIBs. Network Management applications and scripts should convert to the replacement MIBs as soon as possible.

The cable-specific MIBs are described in the following section. For information on the SNMP standard MIBs and Cisco's platform and network-layer enterprise MIBs, see the *Cisco MIB* web page on Cisco.com.

## SNMP and Cable-Specific MIBs

Table 1-14 shows the SNMP and cable-specific MIBs that are supported on the Cisco uBR7200 series universal broadband routers. The table provides a brief description of each MIB's contents and the Cisco IOS software release in which the MIB was initially functional—earlier releases might have had unsupported prototype versions of the MIB; later releases might have added new attributes and functionality. Because of interdependencies, the MIBs must be loaded in the order shown in the table.

Note The names given in Table 1-14 are the filenames for the MIBs as they exist on Cisco's FTP site (ftp://ftp.cisco.com/pub/mibs/ or http://www.cisco.com/public/mibs). Most MIBs are available in both SNMPv1 and SNMPv2 versions; the SNMPv1 versions have *V1SMI* as part of their filenames.

Note MIB files from the Cisco IOS 12.0 SC release train that are no longer supported in the subsequent 12.1 EC, 12.2 XF, or 12.2 BC release trains are not listed in the table below.

*Table 1-14 SNMP and Cable-Specific MIBs Supported on Cisco uBR7200 Series Routers*

| MIB Filename | Description | Introduced in Releases |
|---|---|---|
| SNMPv2-SMI.my<br>SNMPv2-SMI-V1SMI.my | This module specifies the Structure of Management Information (SMI) for SNMPv2, as defined in RFC 1902. | 12.0(6)SC<br>12.1(2)EC<br>12.2(4)XF1<br>(12.2 BC[1]) |
| SNMPv2-TC.my<br>SNMPv2-TC-V1SMI.my | This module defines the textual conventions as specified in RFC 1903. | 12.0(6)SC<br>12.1(2)EC<br>12.2(4)XF1<br>(12.2 BC) |
| SNMPv2-MIB.my<br>SNMPv2-MIB-V1SMI.my[2] | The management protocol, SNMPv2, provides for the exchange of messages that convey management information between the agents and the management stations, as defined in RFC 1907. | 12.0(6)SC<br>12.1(2)EC<br>12.2(4)XF1<br>12.2 BC |

*Table 1-14 SNMP and Cable-Specific MIBs Supported on Cisco uBR7200 Series Routers (continued)*

| MIB Filename | Description | Introduced in Releases |
|---|---|---|
| CISCO-SMI.my<br>CISCO-SMI-V1SMI.my | This module specifies the SMI for Cisco's enterprise MIBs. | 12.0(6)SC<br>12.1(2)EC<br>12.2(4)XF1<br>(12.2 BC) |
| CISCO-TC.my<br>CISCO-TC-V1SMI.my | This module defines the textual conventions used in Cisco's enterprise MIBs. | 12.0(6)SC<br>12.1(2)EC<br>12.2(4)XF1<br>(12.2 BC) |
| IF-MIB.my<br>IF-MIB-V1SMI.my | This module describes generic objects for the Layer 3 network interface sublayers. This MIB is an updated version of MIB-II's *if* table and incorporates the extensions defined in RFC 2233. | 12.1(2)EC<br>12.2(4)XF1<br>(12.2 BC) |
| DOCS-IF-MIB.my<br>DOCS-IF-MIB-V1SMI.my | This module describes the DOCSIS-compliant Radio Frequency (RF) interfaces in cable modems (CMs) and the CMTS, as defined in RFC 2670. | 12.1(2)EC<br>12.2(4)XF1<br>(12.2 BC) |
| DOCS-BPI-MIB.my | This module—available in an SNMPv2 version only—describes the attributes for the DOCSIS-specified Baseline Privacy Interface (BPI) on CMs and the CMTS. | 12.1(2)EC<br>12.2(4)XF1<br>(12.2 BC) |
| CISCO-DOCS-EXT-MIB.my<br>CISCO-DOCS-EXT-MIB-V1SMI.my | This module extends the DOCSIS standard RFI MIB (DOCS-IF-MIB) with Cisco-specific extensions, such as QoS attributes and connection status and other information regarding the CMs and CPE devices supported by the CMTS. | 12.1(2)EC<br>12.2(4)XF1<br>(12.2 BC) |
| CISCO-DOCS-REMOTE-QUERY-MIB.my | This module facilitates SNMP polling of remote CMs on a CMTS. | 12.1(2)EC<br>12.2(4)XF1<br>(12.2 BC) |
| CISCO-CABLE-SPECTRUM-MIB.my<br>CISCO-CABLE-SPECTRUM-MIB-V1SMI.my | This module describes the spectrum management flap list attributes. | 12.1(2)EC<br>12.2(4)XF1<br>(12.2 BC) |

1. The Cisco IOS 12.2 BC release train continues the MIBs and most features introduced in the Cisco IOS 12.2 XF release train.
2. Not supported in the Cisco IOS 12.0 SC release train.

## Circuit Interface Identification MIB

The Circuit Interface Identification MIB feature adds support for a new Cisco enterprise MIB, used to assist in SNMP monitoring of circuit-based interfaces. The Circuit Interface MIB (CISCO-CIRCUIT-INTERFACE-MIB) provides a MIB object that can be used to identify individual circuit-based interfaces (for example, interfaces using ATM or Frame Relay). This user-specified identification will then be returned when linkup and linkdown SNMP traps are generated for the interface.

The Circuit Interface MIB consists of a single table, with each row being a sequence of two objects: Circuit Interface Description (cciDescr) and Circuit Interface Status (cciStatus). The "cciDescr" object is used to identify circuits using a textual description of up to 255 characters specified by the user (note that MIB objects are modified using network management system [NMS] applications, and can not be configured using the Cisco IOS command-line interface).

When the row is created by a user, a value is set for the cciDescr object. The table is indexed by “ifIndex” from the IF-MIB. The “cciStatus” is the “RowStatus” object for the rows in the table. The “cciStatus” object can be set to only two values by the user: “createAndGo(4)”, which creates a new row, and “destroy(6)”, which removes an existing row. If the row is created successfully, the “cciStatus” will be active(1). When creating a new row, the user should set the “cciDescr” object along with the “cciStatus” in a single **snmp set pdu** command. If the row is already active, only the “cciDescr” object can be modified.

The other option is to delete the row first by setting the “cciStatus” to “destroy(6)” and then recreate the row with a new value for “cciDescr”. When creating a new row, the “ifIndex” is validated first. If the “ifIndex” value is not valid, the row is not created and an error code is returned. Similarly, when an interface is deleted and there was a corresponding row in this table, that row will be deleted automatically.

After an identifying description is created for an interface by a user, the description (the “cciDescr” object) will be sent along with the other varbinds as part of linkup and linkdown trap notifications.

For further details, see the CISCO-CIRCUIT-INTERFACE-MIB.my file, available at ftp://ftp.cisco.com/pub/mibs/v2/CISCO-CIRCUIT-INTERFACE-MIB.my.

### cdxCmtsCmOnOffTrapEnable SNMP Object

The following new CLI commands are supported for the “cdxCmtsCmOnOffTrapEnable” object:

[**no**] **cable enable-trap cmonoff-notification**

[**no**] **cable enable-trap cmonoff-interval** <*time 0 to 86400*>

These commands have the following default settings:

**no cable enable-trap cmonoff-notification**

**no cable enable-trap cmonoff-interval**

After the default setting has been changed and the new configuration has been saved, the new configuration will remain active after the CMTS reloads.

### Examples

| | |
|---|---|
| **cable enable-trap cmonoff-notification** | This command enables “cdxCmtsCmOnOffNotification” in the RF MAC interface. Alternatively, you can set the SNMP object “cdxCmtsCmOnOffTrapEnable” to true (1). |
| **no cable enable-trap cmonoff-notification** | This command disables “cdxCmtsCmOnOffNotification” in the RF MAC interface. Alternatively, you can set the SNMP object “cdxCmtsCmOnOffTrapEnable” to false (2). |
| **cable enable-trap cmonoff-interval** <*time 0 to 86400*> | This command sets the interval for “cdxCmtsCmOnOffNotification” sent by the CMTS for one online/offline cable modem state change when “cdxCmtsCmOnOffTrapEnable” is set to true (1). Alternatively, you can set the SNMP object “cdxCmtsCmOnOffTrapInterval” to the same time value. |
| **no cable enable-trap cmonoff-interval** | This command sets the interval “cdxCmtsCmOnOffNotification” to 0 so that “cdxCmtsCmOnOffNotification” will be sent for every online/offline cable modem state change when “cdxCmtsCmOnOffTrapEnable” is set to true (1). Alternatively, you can set the SNMP object “cdxCmtsCmOnOffTrapInterval” to 0. |

Note The default for “cdxCmtsCmOnOffTrapInterval” is 0.

### DOCSIS Ethernet MIB Objects Support (RFC 2665)

For a complete list of MIBs supported by the Cisco uBR7200 Series, refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200rn/index.htm

For descriptions of supported MIBs and how to use MIBs, refer to the *Cisco MIBs* web page on Cisco.com.

### DOCSIS OSSI Objects Support (RFC 2233)

Cisco uBR7200 series routers now support the required objects in RFC 2233 for DOCSIS Operations Support System Interface (OSSI) compliance.

- IF-MIB.my is updated to match RFC 2233.
- The following new object is now supported:
  - ifCounterDiscontinuityTime

For a complete list of MIBs supported by the Cisco uBR7200 Series, refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200rn/index.htm

For descriptions of supported MIBs and how to use MIBs, refer to the *Cisco MIBs* web page on Cisco.com.

### Expression MIB Support of Delta, Wildcarding, and Aggregation

This feature adds support of the Delta, Wildcarding, Delta Wildcarding, and Aggregation features in the Distributed Management Expression MIB (EXPRESSION-MIB) to Cisco IOS software for use by SNMP.

The Delta function enables the Expression MIB to use Delta values of an object instead of absolute values when evaluating an expression. Delta is obtained by taking the difference between the current value of an object and its previous value.

The Wildcarding function of the Expression MIB allows evaluation of multiple instances of an object. This is useful in cases where an expression needs to be applied to all instances of an object. The user need not individually specify all instances of an object in the Expression but only has to set the "expWildcardedObject" in "expObjectTable" to TRUE for the respective object.

Aggregation is performed using the sum function in the Expression MIB. The operand to the sum function has to be a wildcard object. The result of the sum function is the sum of values of all instances of the wildcard object.

For a complete description of Expression MIB functionality, see the *Distributed Management Expression MIB*, Internet-Draft, available through the ITEF at http://www.ietf.org/ids.by.wg/disman.html.

### Cisco Call History MIB Command Line Interface

For a complete list of MIBs supported by the Cisco uBR7200 Series, refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200rn/index.htm

For further descriptions of supported MIBs and how to use MIBs, refer to the *Cisco MIBs* web page.

### RF Interface MIB

For a complete list of MIBs supported by the Cisco uBR7200 Series, refer to the refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200rn/index.htm

For descriptions of supported MIBs and how to use MIBs, refer to the *Cisco MIBs* web page on Cisco.com.

### Multicast Source Discovery Protocol (SDP) MIB

The Multicast Source Discovery Protocol (MSDP) MIB feature adds support in Cisco IOS software for the MSDP MIB. This MIB describes objects used for managing MSDP operations using Simple Network Management Protocol (SNMP). Documentation for this MIB exists in the form of an Internet Draft titled "Multicast Source Discovery Protocol MIB" (draft-ietf-msdp-mib-03.txt) and is available through the Internet Engineering Task Force (IETF) at http://www.ietf.org. For additional information, refer to the *MSDP MIB* feature module on Cisco.com.

### Network Time Protocol (NTP) MIB

The Network Time Protocol (NTP) is used to synchronize timekeeping among a set of distributed time servers and clients. The Cisco NTP MIB enables users to remotely monitor an NTP server using the Simple Network Management Protocol (SNMP), provided the MIB itself is implemented on that server. Use of the NTP MIB to monitor the NTP status of routing devices is accomplished using software on a network management system (NMS). There are no new or modified Cisco IOS software commands associated with this feature.

The Cisco implementation of the NTP MIB is based on NTP version 3 (RFC-1305). The MIB objects are all read-only. SNMP requests are processed by reading the corresponding variables from the NTP subsystem and returning them in the response. The NTP MIB defines a set of NTP server system objects, including an NTP server peers table and an NTP server filter register table.

For complete details on the Cisco implementation of the NTP MIB, refer to the MIB file itself at ftp://ftp.cisco.com/pub/mibs/v2/CISCO-NTP-MIB.my.

### SNMP Enhancements to CISCO-DOCS-EXT-MIB

Commencing with Cisco IOS Release 12.2(4)BC1, the following attributes have been added to CISCO-DOCS-EXT-MIB to provide information about the Unsolicited Grant Service (UGS) allocation on the upstream interfaces:

- "cdxIfUpChannelNumActiveUGS" returns the number of active UGS flows currently allocated on the upstream.
- "cdxIfUpChannelMaxUGSInLastOneHour" returns the maximum number of UGS flows allocated on the upstream in the last hour.
- "cdxIfUpChannelMinUGSInLastOneHour" returns the minimum number of UGS flows allocated on the upstream in the last hour.
- "cdxIfUpChannelAvgUGSInLastOneHour" returns the average number of UGS flows allocated on the upstream in the last hour.
- "cdxIfUpChannelMaxUGSInLastFiveMins" returns the maximum number of UGS flows allocated on the upstream in the last five minutes.
- "cdxIfUpChannelMinUGSInLastFiveMins" returns the minimum number of UGS flows allocated on the upstream in the last five minutes.
- "cdxIfUpChannelAvgUGSInLastFiveMins" returns the average number of UGS flows allocated on the upstream in the last five minutes.

For a complete list of MIBs supported by the Cisco uBR7200 Series, refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200rn/index.htm

For descriptions of supported MIBs and how to use MIBs, refer to the *Cisco MIBs* web page on Cisco.com.

### SNMP Objects for Clear Host, Clear Cable Modem, and Show Current CPEs

Host or cable modems can be cleared using the "cdxCmCpeResetNow" MIB object. The number of current CPEs can be displayed using the "cdxCmtsCmCurrCpeNumber" MIB object.

## SNMP MIBs Changes and Updates in Cisco IOS Release 12.3(9a)BC

Cisco IOS Release 12.3(9a)BC adds the following new MIB support for the Cisco uBR7246VXR router.

- CISCO-CABLE-QOS-MONITOR MIB
- CISCO-CABLE-SPECTRUM-MIB
- CISCO-PROCESS-MIB
- DOCS-IF-MIB
- DOCS-QOS-MIB
- DSG-IF-MIB

For additional information about MIBs for the Cisco CMTS, refer to the following resources on Cisco.com:

- *Cisco CMTS Universal Broadband Router MIB Specifications Guide*
  http://www.cisco.com/univercd/cc/td/doc/product/cable/cmtsmib/
- *SNMP Object Navigator*
  http://www.cisco.com/pcgi-bin/Support/Mibbrowser/unity.pl

### CISCO-CABLE-QOS-MONITOR MIB

Cisco IOS Release 12.3(9a)BC introduces additional features for the CISCO-CABLE-QOS-MONITOR MIB, including the following:

- Clarified the descriptions of a number of objects.
- Added a number of objects in the ccqmCmtsEnforceRuleTable to support DOCSIS 1.1 and DOCSIS 2.0 cable modems and to support peak and off-peak monitoring.
- Added the ccqmCmtsIfBwUtilTable to provide thresholds for downstream/upstream bandwidth utilization.
- Deprecated and removed ccqmCmtsEnfRuleByteCount.

### CISCO-CABLE-SPECTRUM-MIB

Cisco IOS Release 12.3(9) introduces support for the CISCO-CABLE-SPECTRUM-MIB on the Cisco uBR7246VXR universal broadband router, with these additional MIB object enhancements:

- ccsFlapListMaxSize and ccsFlapListCurrentSize SNMP objects provide additional description for cable flap lists.
- Added the ccsCmFlapTable to replace the ccsFlapTable. The new object uses `downstream`, `upstream` and `Mac` as indices to replace the ccsFlapTable object.
- The enhanced ccsSNRRequestTable object provides a table of SNR requests with modified description.
- Added the ccsUpSpecMgmtUpperBoundFreq object to assist with spectrum management on the Cisco CMTS.
- Added the ccsCompliance5 object object.

- Added ccsCmFlapResetNow to reset the flap list for a particular cable modem.
- Updated the descriptions for ccsFlapListMaxSize, ccsFlapListCurrentSize, and ccsSNRRequestTable.

The following objects are also now deprecated:

- ccsFlapPowerAdjustThreshold
- ccsFlapMissThreshold
- ccsFlapResetAll
- ccsFlapClearAll
- ccsFlapLastClearTime

The maximum number of entries in the flap-list was changed from a maximum of 8191 for the entire router, to the following:

- 8191 entries for each Broadband Processing Engine (BPE) cable interface, such as the Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, and Cisco uBR-MC5X20S/U.
- 8191 maximum flap-list entries for all non-BPE cable interfaces, such as the Cisco uBR-MC16C, Cisco uBR-MC16S, and Cisco uBR-MC28C.

Two objects are now used to track the flap list size:

- ccsFlapListMaxSize—Reflects the flap list size, as configured by the **cable flap-list size** command.
- ccsFlapListCurrentSize—Reflects the current size of the flap list for each MAC domain (downstream).

### CISCO-PROCESS-MIB

The CISCO-PROCESS-MIB enables you to monitor CPU and memory utilization for RF cards, cable interface line cards and broadband processing engines on the Cisco CMTS. This information is collected via SNMP.

### DOCS-IF-MIB

The DOCS-IF-MIB (released as RFC 2670) has been updated to conform to the version 5 of the DOCSIS 2.0 RF MIB Specification (draft-ietf-ipcdn-docs-rfmibv2-05.txt).

### DOCS-QOS-MIB

Cisco IOS Release 12.3(9) introduces additional MIB object enhancements for the DOCS-QOS-MIB on the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers:

- Updated with the DOCSIS operations support system interface (OSSI) v2.0-N-04.0139-2.
- The default values of docsQosPktClassIpSourceMask and docsQosPktClassIpDestMask objects are set to 0xFFFFFFFF.

### DSG-IF-MIB

The DSG-IF-MIB defines objects that are used to configure, control, and monitor the operation of the DOCSIS Set-top Gateway (DSG) 1.0 feature on Cisco uBR7200 Series and Cisco uBR10012 routers.

Note The MODULE-IDENTITY for the DSG-IF-MIB is dsgIfMib, and its top-level OID is 1.3.6.1.4.1.9.9.999 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.dsgIfMib). Because this is an experimental MIB, its top-level OID is expected to change when the DSG specifications are finalized.

#### MIB Constraints

The DSG-IF-MIB has the following constraints:

- This is an experimental MIB that can be obsoleted and replaced without prior notice, when the DSG specification is finalized.
- This MIB is supported only in Cisco IOS Release 12.3(9a)BC and later releases. It is not supported for the version of DSG that was implemented in Cisco IOS Release 12.2(15)BC1.
- This MIB is not supported in Cisco IOS Release 12.1 EC.
- This MIB is not supported on Cisco uBR7100 routers.

### SNMP Warm Start Trap

When two Cisco uBR7200 series routers are configured for failover and the active unit fails, the standby unit takes over and becomes the active unit. Whenever this occurs, a Failover Switchover SNMP trap is generated and appears to the SNMP server as a “Warm Start” trap.

Note When a Cisco uBR7200 series router is powered up, an SNMP trap is generated and appears to the SNMP server as a “Cold Start” trap. This functionality is already supported in all Cisco IOS 12.1 EC releases.

## Spectrum Management and Advanced Spectrum Management Features

Spectrum management features, including dynamic upstream modulation were introduced in Cisco IOS Release 12.2(4)XF1, and these continue in the Cisco 12.2 BC release train. These and other features relating to spectrum management are described below:


- Advanced Spectrum Management, page 1-120
- Cable Modulation Profile Default Templates, page 1-120
- Downstream Traffic Shaping, page 1-120
- Dynamic Upstream Modulation, page 1-121
- Guided and Scheduled Spectrum Management, page 1-121
- Input Power Levels, page 1-122
- Spectrum Management Enhancements in Cisco IOS Release 12.3(9a)BC, page 1-122
- Upstream Traffic Shaping, page 1-122


The Cisco uBR7200 Series line cards support varying options that allow service providers to specify different rules the system uses when encountering noise on the cable plant. The primary problem with the upstream system is the ingress of noise, both long-term interference from RF sources such as CB and commercial services, and degradation of the HFC plant. There is also short term sources of noise such as electric appliances or switches that appear a finite number of times for a typical duration of 1 microsecond in length and then go away. These various noise sources affect the Bit Error Rate of the upstream data, and can impact the reliability of two-way services on the plant.

## Advanced Spectrum Management

In addition to other features, Cisco offers advanced spectrum management features for optimal selection of the hop-to frequency (optimal frequency hopping) with the advent of the Cisco uBR-MC16S spectrum management card. The Cisco uBR-MC16S features advanced spectrum management capability that records signal-to-noise (SNR) information from 5-to-42 MHz for each upstream port for the purpose of determining noise level, and to identify potential clear spectrum in the event of the need to initiate a frequency hop. When the number of missed station management messages exceeds a configured threshold, an upstream channel frequency reassignment is initiated. The Cisco uBR-MC16S scans the upstream spectrum and locates a clean, available upstream channel within the defined spectrum group.

Note Clean band is defined as > 29 db SNR for 16 Quadrature Amplitude Modulation (QAM), and > 19 db SNR for Quadrature Phase Shift Keying (QPSK). The SNR calculation is based on the signal power level, noise power level over the desired bandwidth.

If you choose to bypass the existing Cisco uBR-MC16S optimal frequency hopping capability designed to optimize the look-ahead capability of the Digital Signal Processors (DSPs), it is possible enforce guided hopping as used on the Cisco uBR-MCxC and Cisco uBR-MC16E line cards. Cisco does not recommend that you disable the optimal frequency hopping feature of the Cisco uBR-MC16S for normal operations.

In addition to optimal frequency hopping, the Cisco uBR-MC16S can dynamically vary upstream channel widths. By entering an optional second channel width value per upstream port, you can instruct the Cisco uBR-MC16S to hierarchically search for clean upstream channels of 3.2 MHz, 1.6 MHz, 800 kHz, 400 kHz, and 200 kHz width.

For additional information about spectrum management features and their configuration, refer to the chapter titled "Spectrum Management for the Cisco Cable Modem Termination System" in the *Cisco Cable Modem Termination System Feature Guide* on Cisco.com.

## Cable Modulation Profile Default Templates

The cable modulation-profile global configuration command has been enhanced with three new options that provide the ability to quickly create basic modulation profiles using the default values for each burst type. The syntax for the new options is:

**cable modulation-profile** *profile* [ **mix** | **qam-16** | **qpsk** ]

Syntax Description

| | |
|---|---|
| *profile* | Specifies the modulation profile number (1-8). |
| **mix** | Creates a default QPSK/16-QAM mix modulation profile where short and long grant bursts are sent using 16-QAM, while request, request data, initial ranging, and station maintenance bursts are sent using QPSK). The burst parameters are set to their default values for each burst type. |
| **qam-16** | Creates a default 16-QAM modulation profile, where all bursts are sent using 16-QAM. The burst parameters are set to their default values for each burst type. |
| **qpsk** | Creates a default QPSK modulation profile, where all bursts are sent using QPSK. The burst parameters are set to their default values for each burst type. |

## Downstream Traffic Shaping

Downstream traffic shaping (to include Type-of-Service) allows traffic shaping from the CMTS on a DOCSIS downstream channel. Downstream traffic shaping limits surges on output interfaces to reduce downstream congestion or to conform to traffic contract parameters such as PCR.

For additional information about downstream traffic shaping, refer to the following resources:

- "Setting Downstream Traffic Shaping" section on page 3-10
- The "Spectrum Management for the Cisco Cable Modem Termination System" chapter in the *Cisco Cable Modem Termination System Feature Guide* on Cisco.com:

  http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/

## Dynamic Upstream Modulation

The Dynamic Upstream Modulation feature reduces the risks associated with making transition to Quadrature Amplitude Modulation (QAM)-16 in the return path, and provides assurance that subscribers remain online and connected during periods of return-path impairments.

This feature actively monitors the signal-to-noise-ratio (SNR) and forward error correction (FEC) counters in the active return path of each upstream port. The software tracks whether the current upstream channel signal quality can adequately support the higher modulation scheme configured, and adjusts in proactive fashion to the more robust quadrature phase-shift keying (QPSK) modulation scheme when necessary. When return-path spectrum conditions improve, the software returns the upstream channel to the higher-modulation QAM scheme. This is done through modulation profiles supported in Cisco IOS, which can be configured in a variety of ways to support the unique environment at each user's facility.

You can configure Dynamic Upstream Modulation on interfaces with fixed upstream frequencies or on interfaces with spectrum groups assigned. Cisco IOS provides one preconfigured modulation profile resident in memory, which defines a typical profile for QPSK modulation. In order to use the Dynamic Upstream Modulation feature, a second profile must be created that is unique from the first profile and typically provides a higher modulation scheme. The upstream port must be assigned this second modulation profile.

Use the **cable upstream modulation-profile** command in cable interface configuration mode to configure Dynamic Upstream Modulation:

```
Router(config)# cable modulation-profile 2 mix
```

Use the **cable upstream modulation-profile** command in cable interface configuration mode to assign the modulation profile to an upstream port:

**cable upstream** *n* **modulation-profile** <*primary profile-number*> <*secondary profile-number*>

For more information, refer to the *Cisco uBR7200 Dynamic Upstream Modulation* feature module on Cisco.com.

## Guided and Scheduled Spectrum Management

Cisco's initial response to combat upstream ingress was to add frequency agility through software support on the Cisco uBR-MCxxC DOCSIS line cards. Operators configured spectrum groups to select the new upstream frequency based on scheduled frequency hopping or based on guided frequency hopping. Using time scheduled spectrum management, the upstream channel frequency reassignment process is initiated at a configured time of day or week. Using guided frequency hopping, the number of missed station management messages from the cable modems or set top boxes on that upstream exceeding a configured threshold initiates an upstream channel frequency reassignment. All cable modems on the upstream port migrate to the next frequency, using a round robin scheme to select the next available frequency band, with an assigned input power level defined in the spectrum management group. The frequency change occurs rapidly without data loss and minimal latency.

## Input Power Levels

The input power level, power-level-dBmV, is an option in the **cable spectrum-group** command. The option allows you to specify the expected U.S. input power levels on the upstream receivers on the CMTS when the cable modems are hopping from one fixed frequency to another or from one band to another. Each upstream frequency has an associated upstream input power level in dBmV. The power level is the modem transmit power that each spectrum group can use when an upstream frequency change is necessary. The input power level may be set at the time of the frequency hop.

Specifying an input power level is done so that the cable modems do not have to increase or decrease their transmit power with every hop. The cable operator can perform minor power equalizations as a function of frequency. The valid range is -10 to +10dBmV. The power level value should be changed only if you want to change the power level as part of spectrum management. Some cable plants may want to change only the input power level and not the frequency on a daily time schedule.

For information on how to configure input power levels, see the "Setting Input Power Level" section in the *Cisco Cable Modem Termination System Feature Guide* on Cisco.com.

## Spectrum Management Enhancements in Cisco IOS Release 12.3(9a)BC

Cisco IOS Release 12.3(9a)BC introduces enhancements to spectrum management for the Cisco uBR7246VXR router:

- Supports the Cisco Broadband Troubleshooter (CBT) 3.2, page 1-123 (with caveats)
- Supports Subscriber Traffic Management (STM) Version 1.1, page 1-95 (with caveats)

For additional information about CBT 3.2, spectrum management and STM 1.1, refer to the following documents on Cisco.com:

- *Release Notes for Cisco Broadband Troubleshooter Release 3.2*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_command_reference_book09186a0080108e88.html

- *Spectrum Management for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b586.html

- *Subscriber Traffic Management for the Cisco CMTS*

  *http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a00801b17d0.html*

## Upstream Traffic Shaping

This feature allows the cable modem termination system (CMTS) to perform upstream rate shaping on the DOCSIS (Data-Over-Cable Service Interface Specifications) upstream channel.

With traffic shaping, the CMTS can buffer the grants for rate exceeded modems. This grant buffering at the CMTS avoids TCP-related timeouts and retransmits resulting in an improved TCP throughput performance for the rate-exceeded modems. Thus, shaping enables the CMTS to enforce the peak upstream rate for the modem without degrading overall TCP performance for the modem.

When users do not enable the shaping option for upstream rate limiting, the CMTS upstream-rate-policing code drops bandwidth requests from CMs that are found to have exceeded their configured-peak-upstream rate (using different local drop policies). The effect of bandwidth requests (eventually upstream packets) being dropped causes degraded throughput performance of window-based protocols (like TCP) for these rate-exceeded modems because of the timeouts and retransmits that follow.

For additional information about upstream traffic shaping, refer to the "Setting Upstream Traffic Shaping" section on page 3-26 and to *Spectrum Management for the Cisco Cable Modem Termination System* on Cisco.com.

# Testing, Troubleshooting and Diagnostic Features

The Cisco uBR7200 Series supports several troubleshooting and diagnostic features:


- Cable Downstream Frequency Override, page 1-123
- Cable Flap List, page 1-123
- Cisco CMTS Static CPE Override, page 1-124
- Cisco Broadband Troubleshooter (CBT) 3.2, page 1-123
- Fast Fault Detection, page 1-124


## Cable Downstream Frequency Override

Support for the **cable downstream override** command was introduced for the Cisco uBR7200 series routers in the Cisco IOS 12.0 SC, 12.1 EC, and 12.1T release trains.

This command is never needed for normal operations, because downstream frequency override is enabled by default for DOCSIS operations. However, this command can be used to disable the frequency override feature for test and lab use. This override forces the cable modems on that interface to use a particular downstream frequency, regardless of the signal quality.

Additional information about this command and usage guidelines are available in the *Cisco Broadband Cable Command Reference Guide* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm

## Cable Flap List

The flap list is a patented tool that is incorporated in the Cisco IOS software for the Cisco Cable Modem Termination System (CMTS) universal broadband routers for troubleshooting cable modem connectivity problems. The flap list tracks “flapping” cable modems—cable modems that have intermittent connectivity problems—that could indicate a problem with the cable modem or with the upstream or downstream portion of the cable plant.

The flap-list feature does not require any special polling or data transmissions but instead monitors the registration and station maintenance activity that is already performed over any network that conforms to Data-over-Cable Service Interface Specifications (DOCSIS). The CMTS, therefore, collects its flap-list data without creating additional packet overhead and without impacting network throughput and performance. It also supports any cable modem or set-top box (STB) that meets the DOCSIS standard.

Note Although this is a Cisco proprietary CMTS feature, it is compatible with all DOCSIS-compliant cable modems. Unlike other monitoring methods that use the Simple Network Management Protocol (SNMP), the flap list uses zero bandwidth.

For additional flap list information, refer to the chapter titled “Flap List Troubleshooting for the Cisco Cable Modem Termination System” in the *Cisco Cable Modem Termination System Feature Guide* on Cisco.com.

## Cisco Broadband Troubleshooter (CBT) 3.2

Multiple Service Operators (MSOs) provide a variety of services such as TV, video on demand, data, and voice telephony to subscribers. Cable companies provide a variety of services such as TV, video on demand, data, and voice telephony to subscribers. Network Administrators and radio frequency (RF)

technicians need specialized tools to resolve RF problems in the cable plant. Cisco Broadband Troubleshooter 3.2 (CBT 3.2) is a simple, easy-to-use tool designed to accurately recognize and resolve such issues.

Cisco IOS Release 12.3(9a)BC enhances support for the Cisco Broadband Troubleshooter (CBT) Version 3.2 on the Cisco uBR7246VXR universal broadband, with newly supported interoperability for the additional software features.

CBT 3.2 offers the following enhancements on the Cisco uBR7246VXR router:

- CBT 3.2 resolves the former caveat CSCee03388. This enable users to compare an upstream and cable modem on the same trace window.

  Formerly, trace windows could support the selection of up to three upstream or cable modems, but the upstream(s) and cable modems could not be mixed. CBT 3.2 now supports three upstreams or cable modems to be selected and mixed in the trace window.

For additional information about CBT 3.2, spectrum management and STM 1.1, refer to the following documents on Cisco.com:

- *Release Notes for Cisco Broadband Troubleshooter Release 3.2*

  http://www.cisco.com/en/US/products/sw/netmgtsw/ps530/prod_release_note09186a0080293344.html

- *Spectrum Management for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b586.html

- *Subscriber Traffic Management for the Cisco CMTS*

  *http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a00801b17d0.html*

## Cisco CMTS Static CPE Override

The **cable submgmt default** command enables Multiple Service Operators (MSOs) to override network DHCP settings on CPE devices when performing troubleshooting with a laptop computer and console connection to the Cisco universal broadband router.

For additional information about using the **cable submgmt default** command, refer to these documents on Cisco.com:

- *Cisco CMTS Static CPE Override*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/prod_troubleshooting_guide09186a0080284e08.html

- *Cisco Broadband Cable Command Reference Guide*

  http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm

## Fast Fault Detection

Cisco IOS Release 12.2(15)BC1 introduces support for Fast Fault Detection (FFD) on the Cisco uBR7246VXR router. This feature improves performance and convergence times when performing N+1 redundancy switchovers by having the failing line card proactively notify the HCCP control system about its failure. This results in a switchover occurring immediately upon a software fault, reducing the downtime of the card and minimizing any interruptions in the traffic that is flowing across the card.

FFD is automatically used on the Cisco uBR7246VXR router when N+1 redundancy operations are configured. For information on configuring and using N+1 redundancy, see the "N+1 Redundancy for the Cisco CMTS" chapter in the *Cisco CMTS Feature Guide*, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufgnpls1.htm

# Virtual Interfaces

The Cisco uBR7200 Series supports the following virtual interface feature, primarily in the Cisco IOS 12.3 BC release train:

- Virtual Interface Bundling on the Cisco uBR-MC28/U BPE, page 1-125

## Virtual Interface Bundling on the Cisco uBR-MC28/U BPE

Cisco IOS Release 12.3(13a)BC introduces support for virtual interface bundling on the Cisco uBR72046VXR universal broadband router and the Cisco uBR-MC28/U Broadband Processing Engine (BPE).

In prior Cisco IOS releases, cable interface bundling was limited to physical interfaces as master or slave interfaces, and **show** commands did not supply bundle information.

Virtual interface bundling removes the prior concepts of master and slave interfaces, and introduces these additional changes:

- Virtual interface bundling uses *bundle interface* and *bundle members* instead of master and slave interfaces.
- The virtual bundle interface is virtually defined, as with IP loopback addresses, for example.
- Virtual interface bundling supports bundle information in multiple **show ip interface** commands.

Virtual interface bundling prevents loss of connectivity on physical interfaces should there be a failure, problematic online insertion and removal (OIR) of one line card in the bundle, or erroneous removal of configuration on the master interface.

Virtual interface bundling supports and governs the following Layer 3 settings for the bundle member interfaces:

- IP address
- IP helper-address
- source-verify and lease-timer functions
- cable dhcp-giaddr (The giaddr field is set to the IP address of the DHCP client.)
- Protocol Independent Multicast (PIM)
- Access control lists (ACLs)
- Sub-interfaces

Note This virtual interface for the bundle should always remain on (enabled with **no shutdown**), but the Cisco CMTS provides warning messages prior to execution of the **shutdown** command.

For configuration, examples, and general guidelines for virtual interface bundling on the Cisco CMTS, refer to the following documents on Cisco.com:

- *Cable Interface Bundling and Virtual Interface Bundling for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008022eba7.html
- *Virtual Interfaces and Frequency Stacking Configuration on MC5x20S and MC28U Line Cards*

  http://www.cisco.com/en/US/tech/tk86/tk804/technologies_white_paper09186a0080232b49.shtml
- *Virtual Interfaces on the Cisco uBR10-MC5X20S/U Card*

  http://www.cisco.com/en/US/products/hw/modules/ps4969/products_feature_guide09186a00801b17cd.html

# VLAN Features

The Cisco uBR7200 Series support the following VLAN feature:

- HSRP over ISL in Virtual LAN Configurations, page 1-126

## HSRP over ISL in Virtual LAN Configurations

Inter-Switch Link protocol (ISL) is a Cisco protocol for interconnecting multiple switches and maintaining VLAN information as traffic goes between switches. ISL provides VLAN capabilities while maintaining full wire speed performance on Fast Ethernet links in full- or half-duplex mode. ISL operates in a point-to-point environment and will support up to 1000 VLANs. You can define virtually as many logical networks as are necessary for your environment.

For configuration information for Hot Standby Router Protocol (HSRP) over Inter-Switch Link (ISL) protocol, refer to these documents on Cisco.com:

- "*Configuring Routing Between VLANs with Inter-Switch Link Encapsulation*" chapter in the *Cisco IOS Switching Services Configuration Guide*, Release 12.2

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/switch_c/xcprt7/xcdvlisl.htm

# VPN and Layer 2 Tunneling Features

The Cisco uBR7200 Series supports multiple features and functions for virtual private networks (VPNs), to include the following:

- Dynamic SID/VRF Mapping Support, page 1-127
- IP Type-of-Service and Precedence for GRE Tunnels, page 1-127
- IPv6 over L2VPN, page 1-127
- Mapping Service Flows to MPLS-VPN, page 1-128
- MPLS VPN Support for Subinterfaces and Cable Interface Bundles, page 1-128
- Overlapping Subinterface IP Addresses, page 1-129
- Transparent LAN Services (TLS) and L2 Tunneling ATM/SIDs, page 1-130
- Transparent LAN Services (TLS) and L2 Virtual Private Networks, page 1-130

## Dynamic SID/VRF Mapping Support

Cisco IOS release 12.3(13a)BC introduces support for dynamic service ID (SID) and VRF mapping on the Cisco CMTS, to support VoIP with MPLS. Formerly, the MPLS SID mapping feature only applied to provisioned service flows. This feature enables the mapping of all PacketCable DQoS service flows to one particular VRF.

For additional information about dynamic SID to VRF mapping, refer to the following:

- *Mapping Service Flows to MPLS VPN on the Cisco CMTS*

http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_book09186a008019b6bd.html

## IP Type-of-Service and Precedence for GRE Tunnels

Prior to this feature, at generic route encapsulation-based tunnel endpoints, the Type-of-Service (TOS) bits (including precedence bits) were not copied to the tunnel or GRE IP header that encapsulates the inner packet. Instead, those bits were set to zero. This was not a problem unless the intermediate routers between two tunnel endpoints honored TOS or precedence bits, in which case those settings were ignored.

With the advent of virtual private network (VPN) and QoS applications, it is desirable to copy the TOS bits when the router encapsulates the packets using GRE. Thus, intermediate routers between tunnel endpoints can take advantage of the QoS features such as weighted fair queuing (WFQ) and weighted random early detection (WRED).

This feature provides the following benefits:

- Routers between GRE tunnel endpoints will adhere to precedence bits and other TOS bits, thereby possibly improving the routing of important packets. Cisco IOS Quality-of-Service technology, such as policy routing, Committed Access Rate, WFQ, and WRED can operate on intermediate routers between GRE tunnel endpoints.
- Additional security is possible when Cisco IOS network layer encryption is used with precedence for GRE tunnels to provide data confidentiality between VPN tunnel endpoints.
- QoS policy granularity is available per network, per user, and per application.
- The deployment of a GRE tunnel is flexible; it can be applied at the Enterprise CPE or at the Service Provider ingress point.

For configuration information, refer to the following document on CIsco.com:

- *IP Precedence for GRE Tunnels*

http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_4/greqos.htm

## IPv6 over L2VPN

Beginning with Cisco IOS Release 12.3(17a)BC, the Cisco uBR7246VXR router now supports IPv6 using Layer 2 VPNs based on SID to 802.1q mapping. The Cisco uBR7246VXR router already supported Transparent LAN service with Layer 2 VPNs in Cisco IOS Release 12.3(13a)BC and later releases. As more Internet users switch to IPv6, the Cisco IPv6 protocol support helps enable the transition. IPv6 fixes a number of limitations in IPv4, such as limited numbers of available IPv4 addresses in addition to improved routing and network autoconfiguration. This feature allows customers to introduce IPv6 into their network with minimal operational impact.

For additional information about this feature, refer to the following documents on Cisco.com:

- IPv6 Documentation: overview, technology, design and configuration information

  http://www.cisco.com/en/US/tech/tk872/tsd_technology_support_protocol_home.html

## Mapping Service Flows to MPLS-VPN

The Cisco uBR7200 series routers have been providing Managed Access using multiprotocol label switching-virtual private networks (MPLS-VPNs) configured over cable subinterfaces, with each subinterface configured for a specific ISP. Thus, service providers have a manageable way to offer users access to multiple Internet Service Providers (ISPs) over the same physical hybrid fiber-coaxial (HFC) cable network.

This system works very well when all customer premises equipment (CPE) devices behind a cable modem are using the same ISP. However, users are increasingly requesting more complex networks that would allow multiple CPE devices to access different ISPs through the same cable modem.

For example, different users in one household might want to use different PCs to access different ISPs. Another increasingly common situation is that one user requires a secure VPN connection for telecommuting through one ISP, while other users in the household use other computers to access the public Internet through a separate ISP.

The Mapping Service Flows to MPLS-VPN feature enhances this existing MPLS-VPNs support to provide more flexible Managed Access for different ISPs through the same cable modem.

The Mapping Service Flows to MPLS-VPN feature uses DOCSIS 1.1 upstream packet classifiers and service flow IDs (SFIDs) to map individual CPE devices to separate MPLS-VPN interfaces.

In summary, the service provider creates a DOCSIS configuration file for each cable modem that contains:

- Multiple secondary upstream service flows that specify QoS profiles for each CPE device.
- A Vendor Specific QoS Parameter that identifies the MPLS-VPN route to be used for packets using a particular service flow.
- Multiple secondary upstream packet classifiers that specify the MAC address for each CPE device as the Source MAC Address parameter.

The cable modem then downloads the DOCSIS configuration file during its registration process and configures itself for the proper service flows and packet classifiers.

When the cable modem comes online, it begins receiving packets from its CPE devices. The cable modem uses the packet's source MAC address to match the packet to the proper packet classifier, which then identifies the correct SFID to use. The cable modem then transmits the packet to the Cisco uBR7200 series router using this upstream SFID.

The Cisco uBR7200 series router examines the packet to determine its SFID, and then uses the Vendor-Specific QoS Parameter associated with that service flow to route the packet to the appropriate MPLS-VPN interface.

For additional information on the Mapping Service Flows to MPLS-VPN feature, refer to the following document on Cisco.com:

- *Mapping Service Flows to MPLS-VPN on the Cisco uBR7200 Series Router*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122bc/122bc_11/sfidmpls.htm

## MPLS VPN Support for Subinterfaces and Cable Interface Bundles

The Cisco uBR7200 routers offer MPLS VPN support for subinterfaces and cable interface bundles. Using MPLS VPN technology, service providers can create scalable and efficient private networks using a shared hybrid fiber coaxial (HFC) network and Internet protocol (IP) infrastructure.

Using MPLS VPN technology, service providers can create scalable and efficient private networks using a shared hybrid fiber-coaxial (HFC) network and IP infrastructure. The cable MPLS VPN network consists of this infrastructure:

- The multiple service operator (MSO) or cable company that owns the physical infrastructure and builds VPNs for the Internet service providers (ISPs) to move traffic over the cable and IP backbone.
- ISPs that use the HFC network and IP infrastructure to supply Internet service to cable customers.

Each ISP moves traffic to and from a subscriber's PC, through the MSO's physical network infrastructure, to the ISP's network. MPLS VPNs, created in Layer 3, provide privacy and security by constraining the distribution of a VPN's routes to only the routers that belong to its network. Thus, each ISP's VPN is insulated from other ISPs that use the same MSO infrastructure.

An MPLS VPN assigns a unique VPN Routing/Forwarding (VRF) instance to each VPN. A VRF instance consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine the contents of the forwarding table. Each PE router maintains one or more VRF tables. It looks up a packet's IP destination address in the appropriate VRF table, only if the packet arrived directly through an interface associated with that table. MPLS VPNs use a combination of Border Gateway Protocol (BGP) and IP address resolution to ensure security.

Refer to the chapter "Configuring Multiprotocol Label Switching" in the *Cisco IOS Switching Services Configuration Guide*, Release 12.2 on Cisco.com.

## Overlapping Subinterface IP Addresses

Multiprotocol Label Switching (MPLS)-based Virtual Private Networks (VPNs) are created in Layer 3, and provide privacy and security by constraining the distribution of a VPN's routes to those routers that are members of the VPN only, and by using MPLS forwarding. Each ISP's VPN is insulated from all others sharing the HFC and IP-over-cable infrastructure. MPLS VPN enforces traffic separation by assigning a unique VPN Routing/Forwarding (VRF) instance to each VPN. A VRF instance consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what is in the forwarding table.

Cisco IOS Release 12.1(2)EC1 and earlier releases assumed that IP addresses were unique, but it is possible with an MPLS VPN to configure overlapped IP addresses within a VRF. A configuration of overlapped IP addresses could have caused errors. Cisco IOS Release 12.1(3)EC supports a configuration of overlapping IP addresses for subinterfaces. The same IP subnet can now be configured for CPEs on different VRFs using a Cisco uBR7200 series router to configure an MPLS VPN.

The following CLI commands have been updated in recent Cisco IOS releases to support overlapping IP addresses on subinterfaces:

### New CLI Commands

- **cable device** {*ip-address* | *mac-address*} [**no**] **access-group** {*access-list* | *access-name*} | {[**vrf** *vrf-name*] *ip-address* [**no**] **access-group** [*access-list* | *access-name*]}
- **cable host** {*ip-address* | *mac-address*} [**no**] **access-group** {*access-list* | *access-name*} | {[**vrf** *vrf-name*] *ip-address* [**no**] **access-group** [*access-list* | *access-name*]}
- **clear cable host** {*ip-address* | *mac-address*}
- **show cable device** [**vrf** *vrfname*] [*ip-address*] **access-group**
- **show cable host** [**vrf** *vrfname*] [*ip-address* | *mac-address*] **access-group**

Note For the latest command information and detailed command history, refer to the *Cisco Broadband Cable Command Reference Guide* on Cisco.com.

## Transparent LAN Services (TLS) and L2 Tunneling ATM/SIDs

Cisco IOS 12.3(9a)BC introduces support for the Transparent LAN Service over Cable feature on the Cisco uBR7246VXR router. This feature enhances existing Wide Area Network (WAN) support to provide more flexible Managed Access for multiple Internet service provider (ISP) support over a hybrid fiber-coaxial (HFC) cable network.

This feature allows service providers to create a Layer 2 tunnel by mapping an upstream service identifier (SID) to an ATM permanent virtual connection (PVC) or a Virtual Local Area Network (VLAN).

For additional information about configuring TLS on the Cisco uBR7246VXR router, refer to the following document on Cisco.com:

- *Transparent LAN Service over Cable*

http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a0080159396.html

## Transparent LAN Services (TLS) and L2 Virtual Private Networks

Cisco IOS Release 12.3(13a)BC introduces the following changes or requirements for the TLS feature with Layer 2 VPNs:

- When the TLS feature is used with Layer 2 VPNs, the participating cable modems must have the Baseline Privacy Interface security feature (BPI) enabled. Otherwise, the Cisco CMTS drops such Layer 2 traffic in the upstream or downstream.
- Information about Customer Premises Equipment (CPE) does not display in the output of the **show cable modem** command.

Note Configuring ATM L2VPN or 802.1q for a particular cable modem removes any previous cable modem configuration on the Cisco uBR7246VXR router. For example, if TLS with 802.1q is configured on the router for a particular cable modem, and then you configure ATM L2VPN for the same cable modem, the Cisco uBR7246VXR router supports the latter and removes the former with no additional warning or system messages.

Refer to the following documents on Cisco.com for additional TLS information:

- *TLS for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a0080159396.html

- *TLS Over Cable* - TAC Document #60027

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_configuration_example09186a008029160d.shtml

# WAN Optimization and Services Features

The Cisco uBR7200 Series supports multiple WAN features:


- Bandwidth Allocation Control Protocol (BACP), page 1-131
- Closed User Group Selection Facility Suppress Option, page 1-131
- Enhanced Local Management Interface (ELMI), page 1-132
- Frame Relay Enhancements, page 1-132
- Frame Relay MIB Extensions, page 1-132
- Frame Relay Router ForeSight, page 1-133
- ISDN Advice of Charge, page 1-133
- ISDN Caller ID Callback, page 1-133
- ISDN Multiple Switch Types, page 1-134
- ISDN NFAS, page 1-134
- Microsoft Point-to-Point Compression (MPPC), page 1-134
- MLPPP Support, page 1-134
- National ISDN Switch Types for BRI and PRI, page 1-135
- PAD Subaddressing, page 1-135
- PPPoE Termination Support on Cable Interfaces, page 1-135
- VPDN MIB and Syslog Facility, page 1-136
- X.25 Enhancements, page 1-136
- X.25 Switching Between PVCs and SVCs, page 1-136


## Bandwidth Allocation Control Protocol (BACP)

The BACP provides Multilink PPP (MLP) peers with the ability to govern link utilization. Once peers have successfully negotiated BACP, they can use the Bandwidth Allocation Protocol (BAP), which is a subset of BACP, to negotiate bandwidth allocation. BAP provides a set of rules governing dynamic bandwidth allocation through call control; a defined method for adding and removing links from a multilink bundle for Multilink PPP is used.

BACP provides the following benefits:

- Allows multilink implementations to interoperate by providing call control through the use of link types, speeds, and telephone numbers.
- Controls thrashing caused by links being brought up and removed in a short period of time.
- Ensures that both ends of the link are informed when links are added or removed from a multilink bundle.

For configuration information, refer to the chapter titled "Configuring the Bandwidth Allocation Control Protocol" in the *Cisco IOS Dial Services Configuration Guide: Network Services*, Release 12.1 on Cisco.com.

## Closed User Group Selection Facility Suppress Option

A closed user group (CUG) selection facility is a specific encoding element that allows a destination data terminal equipment (DTE) to identify the CUG to which the source and destination DTEs belong. The Closed User Group Selection Facility Suppress Option feature enables a user to configure an X.25 data

communications equipment (DCE) interface or X.25 profile with a DCE station type to remove the CUG selection facility from incoming call packets destined for the preferential CUG only or for all CUGs. You can also remove the selection facility from a CUG with outgoing access (CUG/OA).

## Enhanced Local Management Interface (ELMI)

When used in conjunction with traffic shaping, the router can respond to changes in the network dynamically. The optional Enhanced Local Management Interface (ELMI) feature allows the router to learn QoS parameters from the Cisco switch and use them for traffic shaping, configuration, or management purposes.

ELMI also simplifies traffic shaping configuration on the router. Previously, users needed to configure traffic shaping rate enforcement values, possibly for every VC. Enabling ELMI reduces the chance of specifying inconsistent or incorrect values when configuring the router.

To enable ELMI, you must configure it on the main interface. For configuration information, refer to the chapter titled "Configuring Frame Relay and Frame Relay Traffic Shaping" in the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2 on Cisco.com.

## Frame Relay Enhancements

**Cisco IOS Releases**—Cisco IOS Release 12.2(4)BC1 and the Cisco uBR7200 series support recent frame relay enhancements, such as:

- Frame Relay end-to-end keepalives
- PPP configuration over Frame Relay

For additional information about configuring frame relay, refer to one of these two documents, on Cisco.com, depending on your Cisco IOS release:

- "Configuring Frame Relay" in the *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.1
- "Configuring Frame Relay and Frame Relay Traffic Shaping" in the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2

## Frame Relay MIB Extensions

The Cisco Frame Relay MIB adds extensions to the standard Frame Relay MIB (RFC 1315). It provides additional link-level and VC-level information and statistics that are mostly specific to Cisco Frame Relay implementation. This MIB provides SNMP network management access to most of the information covered by the **show frame-relay** commands, such as **show frame-relay lmi**, **show frame-relay pvc**, **show frame-relay map**, and **show frame-relay svc**.

For additional information, refer to "Configuring Frame Relay" in the *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.2 on Cisco.com.

For a release-specific list of MIBs supported by the Cisco uBR7200 Series, refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200rn/index.htm

For descriptions of supported MIBs and how to use MIBs, refer to the *Cisco MIBs* web page on Cisco.com.

## Frame Relay Router ForeSight

ForeSight is the network traffic control software used in some Cisco switches. The Cisco Frame Relay switch can extend ForeSight messages over a User-to-Network Interface (UNI), passing the backward congestion notification for VCs. ForeSight allows Cisco Frame Relay routers to process and react to ForeSight messages and adjust VC level traffic shaping in a timely manner.

ForeSight must be configured explicitly on both the Cisco router and the Cisco switch. ForeSight is enabled on the Cisco router when Frame Relay traffic shaping is configured. However, the router's response to ForeSight is not applied to any VC until the **frame-relay adaptive-shaping foresight** command is added to the VCs map-class. When ForeSight is enabled on the switch, the switch will periodically send out a ForeSight message based on the time value configured. The time interval can range from 40 to 5000 milliseconds.

For additional information about configuring frame relay, refer to "Configuring Frame Relay" in the *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.2 on Cisco.com.

## ISDN Advice of Charge

ISDN Advice of Charge (AOC) allows users to obtain charging information for all calls during the call (AOC-D) or at the end of the call (AOC-E) or both. Users must have subscribed through their local ISDN network to receive the AOC information from the switch. No router configuration changes are required to retrieve this call charging information.

The ISDN AOC feature also supports, for the AOC-D service, an optional configurable short-hold mode that provides a dynamic idle timeout by measuring the call charging period, based on the frequency of the AOC-D or the AOC-E message from the network. The short-hold mode allows users to track call costs and to control and possibly reduce tariff charges. The short-hold mode idle time will do the following:

- Disconnect a call just prior to the beginning of a new charging period if the call has been idle for at least the configured minimum idle time.
- Maintain the call to the end of the current charging period past the configured idle timeout if the time left in the charging period is longer.

Incoming calls are disconnected using the static dialer idle timeout value.

For configuration information, refer to the chapter titled "Configuring ISDN Special Signalling" in the *Cisco IOS Dial Services Configuration Guide: Terminal Services*, Release 12.1 on Cisco.com.

## ISDN Caller ID Callback

ISDN caller ID callback allows the initial incoming call from the client to the server to be rejected based on the caller ID message contained in the ISDN setup message, and it allows a callback to be initiated to the calling destination.

ISDN caller ID callback allows great flexibility for you to define which calls to accept, which to deny, and which calls to reject initially but for which the router should initiate callback. The feature works by using existing ISDN caller ID screening, which matches the number in the incoming call against numbers configured on the router, determining the best match for the number in the incoming call, and then, if configured, initiating callback to the number configured on the router.

When a call is received, the entire list of configured numbers is checked and the configuration of the best match number determines the action:

- If the incoming number is best matched by a number that is configured for callback, then the incoming call is rejected and callback is initiated.
- If the incoming number is best matched by another entry in the list of configured numbers, the call is accepted.
- If the incoming number does not match any entry in the configured list, the call is rejected and no callback is started.

For configuration information, refer to the chapter titled "Configuring ISDN Caller ID Callback" in the *Cisco IOS Dial Services Configuration Guide: Network Services*, Release 12.1 on Cisco.com.

## ISDN Multiple Switch Types

The Cisco IOS software provides an enhanced *Multiple ISDN Switch Types* feature that allows you to apply an ISDN switch type to a specific ISDN interface and to configure more than one ISDN switch type per router. This feature allows both ISDN BRI and ISDN PRI to run simultaneously on platforms that support both interface types.

For configuration information, refer to the chapter titled "Setting Up Basic ISDN Service" in the *Cisco IOS Dial Services Configuration Guide: Terminal Services*, Release 12.1 on Cisco.com.

## ISDN NFAS

ISDN Non-Facility Associated Signalling (NFAS) allows a single D channel to control multiple PRI interfaces. A backup D channel can also be configured for use when the primary NFAS D channel fails.

For configuration information, refer to the chapter titled "Configuring ISDN Special Signalling" in the *Cisco IOS Dial Services Configuration Guide: Terminal Services*, Release 12.1 on Cisco.com.

## Microsoft Point-to-Point Compression (MPPC)

In March of 1997, Microsoft Corporation introduced the Microsoft Point-to-Point Compression (MPPC) scheme as a means of representing arbitrary PPP packets in a compressed form. MPPC was ratified by the Internet Engineering Task Force (IETF) and is known as RFC 2118. The Windows 95 client software supports both MPPC and LZS Stacker compression, whereas the Microsoft NT server and Windows 2000 only support MPPC, which is negotiated during the Compression Control Protocol (CCP) process.

To enable MPPC compression on access servers, you need to be running Cisco IOS Software version 11.3T or later. Refer to these two documents on Cisco.com for additional information:

- *MPPC Compression on Access Servers*
- *Microsoft Point-to-Point Compression (MPPC)*

## MLPPP Support

The Cisco IOS Multilink Point-to-Point Protocol (MLPPP) feature is now supported for selected line cards and port adapters on the Cisco uBR7100 series and the Cisco uBR7200 Series, which share the same MLPPP code as the Cisco 7200 series. There is no new hardware or software for MLPPP in this release.

Note MLPPP combines one or more physical interfaces into a virtual "bundle" interface. The bandwidth of the bundle interface is equal to the sum of the component links' bandwidth. This allows service providers to make the step from T1 and E1 lines to affordable T3 and E3 speeds.

MLPPP is configured not on a cable interface, but on the T1/E1 link.

### Line Cards and Port Adapters Supporting MLPPP on the Cisco uBR7200 Series

Table 15 lists the line cards and port adapters on the Cisco uBR7200 Series, in conjunction with the applicable network processing engine (NPE), that are supported for MLPPP at the time Cisco IOS Release 12.3(13a)BC was released.

*Table 15 Line Cards and Port Adapters Supporting MLPPP on the Cisco uBR7200 Series for Cisco IOS Release 12.3(13a)BC*

| Model | NPE | Line Card | Port Adapter |
|---|---|---|---|
| Cisco uBR7246VXR | NPE-400, NPE-G1 | MC16C, MC16S, MC28C, MC28U | PA-4T+, PA-MC-2E1/120, PA-MC-4T1 |
| Cisco uBR7114 | N/A | N/A | PA-4E1G/120, PA-4T+, PA-MC-4T1 |

## National ISDN Switch Types for BRI and PRI

The Cisco uBR7200 series supports many national ISDN switch types, including those that support Basic Rate Interface (BRI) and Primary Rate Interface (PRI). ISDN switch types are described further in the document titled *ISDN Switch Types, Codes, and Values* on Cisco.com.

## PAD Subaddressing

In situations where the X.121 calling address is not sufficient to identify the source of the call, you can append a specified value to the calling address using the PAD subaddressing feature. PAD subaddressing allows you to create unique X.121 calling addresses by including either a physical port number or a value specified for a line as a subaddress to the X.121 calling address.

PAD subaddressing enables an X.25 host application to uniquely identify the source of an X.121 call. For example, in some bank security alarm applications, the central alarm host identifies the physical location of the alarm units from subaddressing information contained in the Call Request packet.

For additional information, refer to "Configuring the Cisco PAD Facility for X.25 Connections" in the *Cisco IOS Terminal Services Configuration Guide*, Release 12.2 on Cisco.com.

## PPPoE Termination Support on Cable Interfaces

Cisco IOS Release 12.2(4)BC1 adds support for Point-to-Point Protocol over Ethernet (PPPoE) by allowing a direct connection to cable interfaces. PPPoE provides service-provider digital-subscriber line (DSL) support. The support of PPPoE on cable interfaces of the Cisco uBR7200 series routers allows customer premises equipment (CPE) behind the cable modem to use PPP as a mechanism to get their IP addresses and use it for all subsequent data traffic, just like a dial-up PPP client. In a PPP dial-up session, the PPPoE session is authenticated and the IP address is negotiated between the PPPoE client and the server, which could be either a Cisco uBR7200 series router or a Home Gateway.

Additional information about configuring PPPoE is available in the following documents:

- *Configuring Broadband Access: PPP and Routed Bridge Encapsulation* chapter of the *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.2 on Cisco.com
- Cisco *PPPoE on Ethernet* feature module on Cisco.com
- *RFC 2516*

## VPDN MIB and Syslog Facility

For a complete list of MIBs supported by the Cisco uBR7200 Series, refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200rn/index.htm

For descriptions of supported MIBs and how to use MIBs, refer to the *Cisco MIBs* web page on Cisco.com.

## X.25 Enhancements

X.25 packet-switched support is provided by the operating software that is bundled with the Cisco IOS software image. The operating software provides both the link- and packet-level facilities of the 4T+ port adapter.

The operating software is accessed via a VT100 terminal connected to the console port of the Input/Output controller. The settings of the terminal should be as follows:

Baud: 9600
Data bits: 8
Parity: none
Stop bits: 1

To boot the software from Flash memory, type the following command at the ">" prompt:

```
Router> b flash
```

## X.25 Switching Between PVCs and SVCs

To configure PVC to SVC switching between two serial interfaces, both interfaces must already be configured for X.25. In addition, X.25 switching must be enabled using the x25 routing global configuration command. The PVC interface must be a serial interface configured with X.25 encapsulation. (The SVC interface may use X.25, XOT, or CMNS.)

Use the following command in interface configuration mode once the interfaces have been configured for X.25 switching to configure X.25 switching between PVCs and SVCs:

| Command | Purpose |
|---|---|
| **x25 pvc** *number1* **svc** *x121-address* [*flow-control-options*] [*call-control-options*] | Configures PVC traffic to be forwarded to an SVC. |

To display information about the switched PVC to SVC circuit, use the following command in privileged EXEC mode:

| Command | Purpose |
|---|---|
| **show x25 vc** [**lcn**] | Displays information about the active SVCs and PVCs. |

For additional information, refer to the chapter titled "*Configuring X.25 and LAPB*" in the *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.2 on Cisco.com.

Note Early deployment releases contain fixes to software caveats as well as support for new Cisco hardware and software features

# DOCSIS and CMTS Interoperability

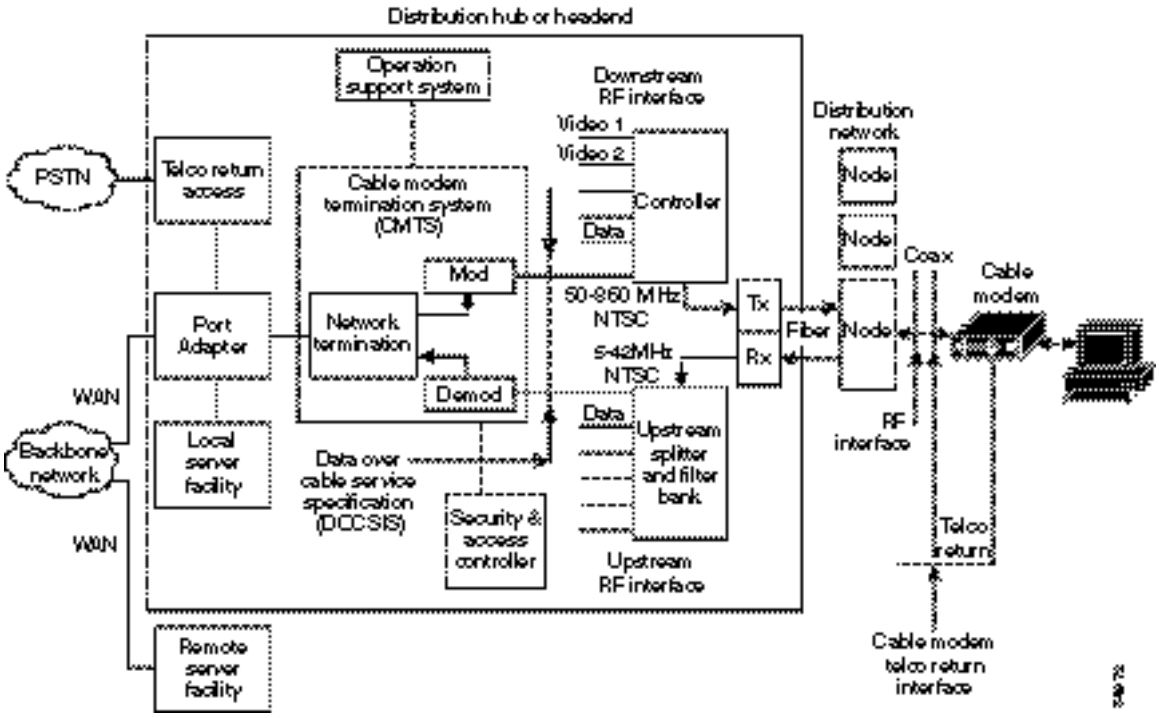
This section contains the following topics to familiarize you with DOCSIS architectural fundamentals:


- "DOCSIS NTSC Cable Plants" section on page 1-137
- "EuroDOCSIS Cable Plants" section on page 1-138
- "DOCSIS-Compliant Downstream Signals" section on page 1-139
- "DOCSIS-Compliant Upstream Signals" section on page 1-140
- "Traffic Engineering" section on page 1-142


## DOCSIS NTSC Cable Plants

DOCSIS-compliant cable plants that support North American channel plans use ITU J.83 Annex B RF. Figure 1-1 illustrates a DOCSIS two-way and telco-return architecture.

*Figure 1-1 DOCSIS Two-Way and Telco-Return Architecture*



Larger cable companies typically have high-speed fiber backbones that carry Internet data, voice, and video between the following cable company facilities:

- Regional processing centers
- Headends
- Hubs

The fiber backbone can be made up of OC-3 (155 Mbps) to OC-48 (2488 Mbps) Synchronous Optical Network (SONET) or Asynchronous Transfer Mode (ATM) rings. The backbone network can connect to other networks, including the Public Switched Telephone Network (PSTN), other cable system backbones, or to public Internet interconnect points that multiple ISPs use.

The CMTS Media Access Control (MAC) domain typically includes one or more downstream paths and one or more upstream paths. Depending on the CMTS configuration, the CMTS MAC domain can be defined to have its downstreams on one cable interface line card with its upstreams on another card, or one or more CMTS MAC domains per cable interface line card.

Cisco provides high-speed routers to route interactive traffic between the backbone and Ethernet in the headend internal network. Signaling protocols maintain the network intelligence needed to route traffic optimally, automatically building and maintaining routing tables to direct traffic and signal failures for rerouting in the network.

Border Gateway Protocol (BPG) typically operates between the cable operator's regional network and external networks, providing routing information exchange between different networks. The Open Shortest Path First (OSPF) protocol is used in regional networks usually. Cisco routers incorporate Cisco IOS software, which offers advanced software features, including quality of service (QoS), Weighted Fair Queuing (WFQ), and IP multicast.

## EuroDOCSIS Cable Plants

EuroDOCSIS-based cable plants use EuroDOCSIS J.112 (Annex A) standard, similar to the DAVIC/DVB J.83 Annex A physical layer. The MC16E builds on the DOCSIS protocol, adding support at the physical layer for PAL and SECAM channel plans. The card permits full bandwidth utilization of the 8 MHz downstream channel, allowing up to 50 Mbps throughput, and greater upstream frequency selection—5 to 65 MHz, instead of 5 to 42 MHz.

Figure 1-2 illustrates a three-tier EuroDOCSIS configuration involving STB deployment. The sample architecture has four subsystems:

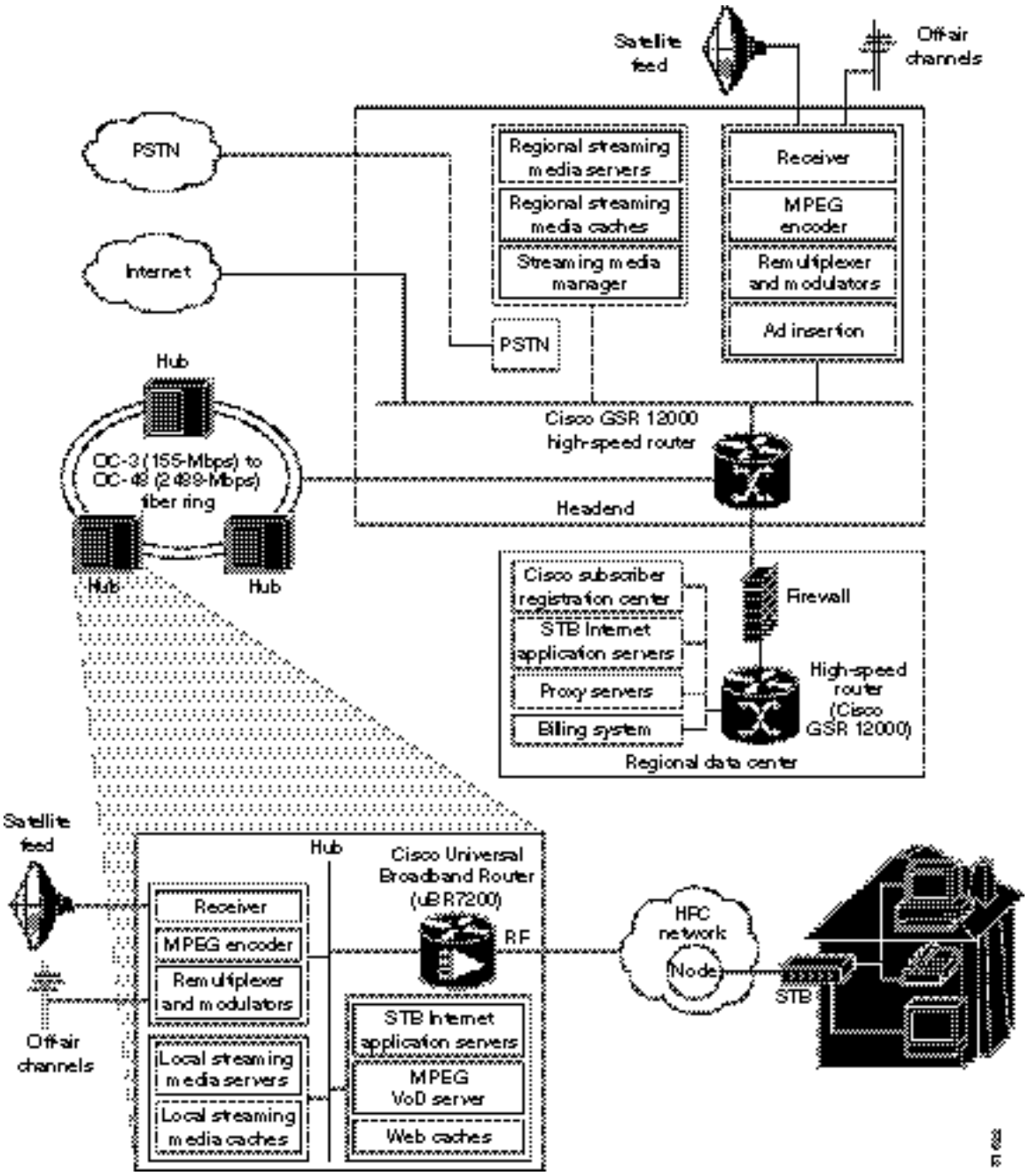
- High-speed fiber backbone—Carries Internet data, voice, and video between regional processing centers, headends, and hubs.
- Headend—Aggregates content at the national and regional level and sends it to the fiber backbone.
- Hub—Combines regional programming with local content and sends that combined content to the cable network.
- Interactive STBs with integrated EuroDOCSIS CMs—Connects subscribers to the cable network.

Video sources are Motion Picture Experts Group (MPEG) encoded and then fed into an MPEG multiplexer that packs the MPEG video streams into a single stream. This stream is uplinked to a satellite and then downlinked to multiple headends, which then distribute the MPEG stream directly onto the HFC plant.

The STB receives signals from the cable network and displays them on a television. An STB with EuroDOCSIS cable modem functionality supports two-way interactivity. Inside the EuroDOCSIS STB are two tuners:

- One handles MPEG-2 video, audio, broadcast control data, and broadcast service data.
- The other supports DOCSIS IP data. The return path is implemented with EuroDOCSIS.

*Figure 1-2 EuroDOCSIS and STB Architecture*




# DOCSIS-Compliant Downstream Signals

Downstream signals are modulated using 64 or 256 Quadrature Amplitude Modulation (QAM-64 or QAM-256), based on the cable interface card used, your cable plant, and the significance of the data. DOCSIS defines the messages and data types for CMTS to cable modem (or cable modem in an STB)

communications. All CMs listen to all frames transmitted on the downstream channel on which they are registered and accept those where the destinations match the units themselves or the devices each supports.

The Cisco uBR7200 series supports multicast groups using standard protocols such as Protocol Independent Multicast (PIM), Distance Vector Multicast Routing Protocol (DVMRP), and Internet Group Management Protocol (IGMP) to determine if multicast streams are to be forwarded to a prescribed downstream cable modem or STB, or a multicast routing peer.

The Cisco uBR7200 series software periodically sends MAC allocation and management messages—known as MAPs—to all CMs on the network, defining the transmission availability of channels for specific periods of time. The MAP rate is fixed—every 2 msec.

Different transmission intervals are defined that associate an interval with a Service Identifier (SID). SIDs define the devices allowed to transmit and provide device identification and class of service management. Software defines what type of transmission is allowed during the interval.

The CMTS system administrator typically assigns one or more SIDs to each cable modem, corresponding to the classes of service the cable modem requires. Each MAP is associated with a particular upstream channel. The SID concept supports multiple data flows and use of protocols such as Resource Reservation Protocol (RSVP) that allows IP backbone QoS features to be extended to the CMTS. The CMTS schedules the times granted for sending and receiving packets, and if defined, manipulates the Type-of-Service (ToS) field in the IP packet header to accommodate QoS.

Note Cisco uBR7200 Series software supports extensions to DOCSIS 1.0 to operate with DOCSIS 1.0-based CMs or cable RF CPE devices (such as Cisco uBR924 cable access routers or Cisco uBR910 series cable data service units) that also support DOCSIS 1.0 extensions.

Tip DOCSIS 1.0 extensions address the problem of QoS for VoIP until DOCSIS 1.1 is solidified. Currently, only certain vendors offer products that support DOCSIS 1.0 extensions.

DOCSIS 1.0 extensions build intelligence into the MAP file the CMTS sends to voice-enabled CMs to address jitter and delay. The extensions support unsolicited grants, allowing a portion of bandwidth to be dedicated to a voice call as soon as a subscriber initiates a call until that call is terminated. Unsolicited grants are used to create a constant bit rate-like stream between the CMTS and the cable modem, in contrast to typical data applications where CMs request grants from the CMTS before they can transmit upstream. Refer to the "This section summarizes Cisco uBR7200 series router software features for all supported Cisco IOS Release trains, and directs you to additional configuration information for each feature." section on page 1-22 for feature descriptions and links to configuration information.

# DOCSIS-Compliant Upstream Signals

The upstream channel is characterized by many CMs (or CMs in STBs) transmitting to the CMTS. These signals typically operate in a burst mode of transmission. Time in the upstream channel is slotted.

The CMTS provides time slots and controls the usage for each upstream interval. The CMTS sends regular mappings of minislot structure in downstream broadcast MAP messages. The CMTS allocates contention broadcast slots that all CMs can use, and also allocates upstream minislots for unicast or non-contention data from specific CMs.

The CMTS allocates two basic types of contention slots on the upstream:

- Initial ranging slots that CMs use during their initialization phase to join the network. Once the CMTS receives an initial ranging request from a cable modem using this kind of slot, it subsequently polls the cable modem, along with other operational CMs, in unicast, non-contention station maintenance slots.
- Bandwidth-request minislots that CMs use to request data grants from the CMTS to send data upstream in non-contention mode. Any cable modem can use this type of minislot to request a data grant from the CMTS.

The stream of initial ranging slots and bandwidth request minislots comprise two separate contention subchannels on the upstream. Cisco uBR7200 Series software uses a "dynamic bandwidth-request minislots-per-MAP" algorithm to dynamically control the rate of contention slots for initial ranging and bandwidth-requests. The CMTS uses a common algorithm to vary backoff parameters that CMs use within each of the two upstream contention subchannels. The CMTS uses these algorithms to dynamically determine the initial ranging slots and bandwidth-request minislots to allocate on the slotted upstream.

When power is restored after a catastrophic power failure, a large number of CMs will want to join the network simultaneously. This represents an impulse load on the initial ranging subchannel. The CMTS in this situation will increase the frequency of initial ranging slots so that CMs can quickly join the network.

During high upstream data loads, the CMTS conserves the scarce upstream channel bandwidth resource and is more frugal in introducing upstream initial ranging slots. The CMTS schedules bandwidth-request minislots at low loads to provide low access delay. At high upstream loads, the CMTS reduces the number of contention-based request minislots in favor of data grants, while maintaining a minimum number of request slots.

Note The system default is to have the automatic dynamic ranging interval algorithm enabled, automatic dynamic ranging backoff enabled, and data backoffs for each upstream on a cable interface. Commands to configure the dynamic contention algorithms include:
[**no**] **cable insertion-interval** [*automatic* [<*Imin* [*Imax*]>] *in msecs*
[**no**] **cable upstream** <*port number*> **range backoff** [*automatic*] | [<*start*> <*end*>]
[**no**] **cable upstream** <*port number*> **data-backoff** [*automatic*] | [<*start*> <*end*>]

Caution In general, Cisco discourages adjusting default settings. Only personnel who have received the necessary training should attempt to adjust values.

The Cisco uBR7200 series equipment periodically broadcasts Upstream Channel Descriptor (UCD) messages to all CMs. These messages define upstream channel characteristics that include upstream frequencies, symbol rates and modulation schemes, Forward Error Correction (FEC) parameters, and other physical layer values.

Upstream signals are demodulated using Quadrature Phase Shift Keying (QPSK) or Quadrature Amplitude Modulation (QAM). QPSK carries information in the phase of the signal carrier, whereas QAM uses both phase and amplitude to carry information.

Tip If your cable plant is susceptible to ingress or noise, QPSK is recommended based on the importance of the data. Frequencies below 20 MHz are more susceptible to noise and might require lower symbol rates. Higher frequencies might be able to support higher rates and use QAM modulation instead.

# Traffic Engineering

Sending data reliably upstream is a critical issue. Designing a robust upstream architecture requires balancing system parameters, establishing subscriber data requirements, and configuring the network to support those requirements.

Upstream spectrum varies greatly between cable plants. Maintaining stable return paths also differs based on varying patterns and levels of ingress noise and interference. Common problems in cable plants include:

- Electrical and magnetic interference (EMI)
- Thermal noise
- Carrier to noise (C/N) imbalances
- Interference of leaking signals
- Ingress due to other channels appearing at the desired channel frequency
- Distortion due to non-linearities of cable equipment
- Cross modulation—carrier to frequency distortion
- Hum and low frequency distortion
- Improper RF amplifier tuning
- Non-unity gains due to incorrect usage of attenuators
- Low-quality subscriber equipment
- Out of range signal power from the CMTS to the cable modem

When configuring your system, configure downstream and upstream parameters based on the fiber nodes involved, the required services the cable modem or STB supports, the importance of the data, and desired performance capabilities.

Your cable plant determines its data performance. Design your network to maximize its performance and capacity at minimum cost, while meeting subscriber data requirements. Select or customize upstream profiles for maximum trade-offs between bandwidth efficiency and upstream channel robustness once you're familiar with the system and have characterized your network. For example, QAM-16 requires approximately 7 dB higher C/N ratio to achieve the same bit error rate (BER) as QPSK, but it transfers information at twice the rate of QPSK.

Note Older plants and plants with long amplifier cascades are more susceptible to ingress than newer plants. These plants produce more noise and signal level variances.

Tip Cisco recommends you keep input to all amplifiers at the same power level in the upstream direction and keep output of all amplifiers in the downstream direction at the same power level. This is called unity gain. Tune amplifiers and other equipment properly at desired frequencies. To characterize and improve your cable plant's stability, follow procedures in the *Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide* on Cisco.com.

A DOCSIS cable plant has the following groups of traffic to size based on current service offerings:

- Basic Internet access data, which is burst-intensive and asymmetrical; asymmetrical traffic supports a larger data rate in one direction—the downstream.

- VoIP traffic, which requires constant bandwidth, has low tolerance to latency and jitter, and is typically symmetrical—supporting the same data rate in downstream and upstream directions. VoIP generally requires phase-lock and jitter attenuation.
- VPN traffic, which requires secure transmissions; traffic is typically symmetrical since telecommuters exchange more data upstream than residential Internet access customers.
- Video, which can include digital video channels based on the services in your network; current Cisco uBR7200 Series products support EuroDOCSIS operation where data is MPEG encoded and packed into an 8 MHz RF channel spacing based on the channel plan used and equipment at the headend or distribution hub. Video flows in one direction and control information flows in the other.
- Signaling and maintenance—the DOCSIS MAC layer support includes DOCSIS encapsulation, initial maintenance, station maintenance, registration, frequency hop, and upstream channel changes.

You have a wide range of options to engineer your network. Define your network based on your cable facilities—headend or distribution hub—and your anticipated service offerings, subscription, and required service levels. Define data requirements relative to the number of subscribers to support and their usage patterns. Select upstream symbol rate, modulation format, and other parameters based on data requirements and return path characterizations.

If the service is asymmetrical, determine the ratio of downstream to upstream data rates. For basic Internet access where the majority of traffic is sent to a subscriber and the subscriber sends only a small amount of data upstream, use ratios ranging from 5:1 to 10:1.

Determine what data rate the service should support. Define the maximum and minimum data rate, answering the following questions:

- Do you want to define the minimum data rate relative to the maximum?
- Will the minimum data rate equal the maximum?
- Will it be a percentage of the maximum?
- Will the minimum data rate be zero?

**Note** The minimum data rate has the greatest impact on the network. The network must be sized to accommodate this level of traffic to fulfill the defined service data requirements. The amount of bandwidth available to a group of subscribers establishes where, within the defined maximum and minimum data rates, a subscriber within a group is able to operate.

For video traffic planning purposes, use a typical bit rate to calculate densities of video streams within a channel. For QoS calculations, limit the number of video streams per channel to prevent packet drops. The key traffic parameter is how many IP video streams will fit into the RF channel.

Ideally, the network is sized so that it supports all subscribers being active at the same time at the maximum data rate. This results in an expensive network, however, where full capacity, particularly for residential subscribers, is rarely used. Cisco recommends designing your network to support a given level of over-subscription.

**Note** Configure your network to support a percentage of all subscribers at a given data rate. At this level, the network supports the bandwidth needs of all active users. Provided the over-subscription rate is low enough, such that service definitions are met, all subscribers receive the service to which they subscribed.

**Caution** With over-subscription, the network is unable to support all subscribers being active at the maximum data rate. If the over-subscription is severe enough, subscribers may be denied service.

Parameters to determine the over-subscription level include:

- Peak percentage of simultaneous users—Not all subscribers access the network at the same time. Subscribers have different access patterns that vary based on profiles; working hours; family demographics; type of user—telecommuter or residential Internet access customer. Only a portion of subscribers are active at a given time. This number serves as the “peak percentage of simultaneous users parameter”— busy hour number of subscribers.
- Average data rate per subscriber—Not only are all subscribers not active at the same time, but they do not continuously operate at peak rate. Using basic Internet access as an application, data that subscribers request and send downstream and upstream is burst-intensive. A group of subscribers, therefore, has an average data rate less than the maximum rate defined by the service.

Note For some services, the average value might be the maximum rate. VoIP is such an application.

How bandwidth contention is handled depends on the mix of services defined and individual service definitions.

Percentage of homes passed subscribing to the service is another factor to consider. If this parameter is set too conservatively, the network is under-engineered and requires modification to grow the service. If set too aggressively, the network is over-engineered and costs for services are higher than they should be.

Full implementation of service levels requires additional higher layer items including scheduling, queuing priorities, bandwidth allocation. These items are addressed in DOCSIS 1.0 extensions. Refer to the “This section summarizes Cisco uBR7200 series router software features for all supported Cisco IOS Release trains, and directs you to additional configuration information for each feature.” section that follows and respective chapters of this guide for additional information.

Note For detailed engineering calculations, refer to the Cisco *Multimedia Traffic Engineering for HFC Networks* white paper publication on Cisco.com.

# Configuring the Cable Modem Termination System for the First Time

This chapter describes how to start up and configure the Cisco uBR7200 series Cable Modem Termination System (CMTS) for the first time. This chapter contains the following sections:

| Section | Purpose |
|---|---|
| "Configuration Fundamentals for the Cisco uBR7200 Series" section on page 2 | Identifies tasks and analysis that you must complete prior to powering on and configuring the Cisco uBR7200 series router. This includes instructions for completing preconfiguration tasks and for using password procedures. |
| "Configuring the Cisco uBR7200 Series Using AutoInstall" section on page 10 | Describes how to use the AutoInstall process, which is designed to configure the Cisco uBR7200 series router automatically *after* connection to your WAN. |
| "Configuring the Cisco uBR7200 Series Using the Setup Facility" section on page 17 | Describes how to use the Setup facility (also called the System Configuration dialog) for configuring your CMTS, an alternative to AutoInstall. Use the Setup facility *prior to* completing a WAN or LAN connection to your router. The Setup facility supports several functions so that cable interfaces and cable interface line cards are fully operational (after initial setup). |
| "Configuring the Cable Interface with the Extended Setup Facility" section on page 25 | Provides instructions for using the Setup facility to create an initial configuration. The extended setup prompts you to configure each interface on the system. |
| "Configuring the Cisco uBR7200 Series Manually Using Configuration Mode" section on page 27 | Describes how to configure the Cisco uBR7200 series router manually if you prefer not to use the Setup or AutoInstall facilities. |
| "Saving Your Configuration Settings" section on page 29 | Describes how to store the configuration or changes to your startup configuration in NVRAM using the **copy running-config startup-config** command. |
| "Reviewing Your Settings and Configurations" section on page 29 | Provides commands to check your settings and review any changes to your configuration. |
| "Overview of the Cisco Network Registrar for the Cisco uBR7200 Series" section on page 1 | Provides additional cable-specific instructions about the Cisco Network Registrar (CNR) that are pertinent to the Cisco uBR7200 series and CMTS management. |

Note These sections provide minimal configuration instructions. For additional configuration information, refer to subsequent chapters in this guide. For examples of Cisco uBR7200 series CMTS configuration files, refer to the "Viewing Sample Configuration Files" section on page 29.

Additional feature configuration information is available in these documents on Cisco.com:

- *Cisco Cable Modem Termination System Feature Guide*
- *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.1
- *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.1

Tip Be sure that you have appropriate addresses and values based on your network before you attempt to configure the router. Enter the **show version** command to display the release of Cisco IOS software on your router.

# Configuration Fundamentals for the Cisco uBR7200 Series

This section describes the basic parameters of using passwords, and describes initial configuration utilities that are available to you. This section contains the following topics:

- Preconfiguring the Cisco uBR7200 Series, page 2
- Booting and Logging onto the Cisco uBR7200 Series, page 5
- Setting Password Protection on the Cisco uBR7200 Series, page 5
- Recovering Passwords on the Cisco uBR7200 Series, page 6

## Preconfiguring the Cisco uBR7200 Series

Complete these prerequisite steps before you power on and configure the Cisco uBR7200 series router:

SUMMARY STEPS

1. Ensure that your network supports reliable broadband data transmission.
2. Ensure that your Cisco uBR7200 series router is installed in operational fashion.
3. Ensure that all other required headend or distribution hub routing and network interface equipment is installed, configured, and operational (based on the supported services).
4. Ensure that DHCP and DOCSIS configuration files have been created and pushed to appropriate servers.
5. Verify sufficient and proper CPE.
6. Be familiar with your channel plan to assign appropriate frequencies.
7. Be familiar with your dial plan.
8. Obtain additional IP and security information as necessary.

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | Ensure that your network supports reliable broadband data transmission. | Your plant must be swept, balanced, and certified based on National Television Standards Committee (NTSC) or appropriate international cable plant recommendations.<br>Ensure that your plant meets all Data-over-Cable Service Interface Specifications (DOCSIS) downstream and upstream radio frequency (RF) requirements. These requirements are documented in the DOCSIS RF Specifications:<br>http://www.cablemodem.com/specifications.html<br>Configuration information for downstream and upstream interfaces is contained in Chapter 3, "Configuring Cable Modem Interface Features." |
| Step 2 | Ensure that your Cisco uBR7200 series router is installed in operational fashion. | Ensure that your Cisco uBR7200 series router is installed according to the instructions in the hardware installation guide that came with your CMTS (for example, the *Cisco uBR7200 Series Hardware Installation Guide* on Cisco.com:<br>http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cr72hig/index.htm |
| Step 3 | Ensure that all other required headend or distribution hub routing and network interface equipment is installed, configured, and operational (based on the supported services). | Headend installation requirements include:<br>• All routers<br>• Servers (Dynamic Host Configuration Protocol (DHCP), TFTP, and time-of-day (ToD))<br>• Network management systems<br>• Other configuration or billing systems<br>• IP telephony equipment including gatekeepers and gateways<br>• Backbone and other equipment if supporting VPN<br>Dial-up access servers, telephone circuits/connections and other equipment if supporting telco return |
| Step 4 | Ensure that DHCP and DOCSIS configuration files have been created and pushed to appropriate servers. | When initialized, each cable modem should be enabled to perform the following tasks:<br>• Transmit a DHCP request<br>• Receive an IP address<br>• Obtain TFTP and ToD server addresses<br>• Download a DOCSIS configuration file or updated software image if using Cisco uBR924 cable access routers or Cisco uBR910 cable data service units (DSUs) in your network. |

| | Command or Action | Purpose |
|---|---|---|
| Step 5 | Verify sufficient and proper CPE. | Ensure that customer premises equipment (CPE)—CMs or set-top boxes (STBs), PCs, telephones, or facsimile machines—meet requirements for your network and service offerings. |
| Step 6 | Be familiar with your channel plan to assign appropriate frequencies. | Outline your strategies for setting up bundling or VPN solution sets, if applicable to your headend or distribution hub. |
| Step 7 | Be familiar with your dial plan. | Know your dial plan if using H.323 for VoIP services and setting up VoIP-enabled CM configuration files. |
| Step 8 | Obtain additional IP and security information as necessary. | As appropriate, obtain:<br>• Passwords<br>• IP addresses<br>• Subnet masks<br>• Device names |

After these prerequisites are met, you are ready to configure the Cisco uBR7200 series CMTS. This includes, at a minimum:

- Configuring a host name and password for the Cisco uBR7200 series router
- Configuring the router to support IP over the cable plant and network backbone

Caution If you plan to use service-class-based provisioning, the service classes must be configured at the CMTS before CMs attempt to make a connection.

# Booting and Logging onto the Cisco uBR7200 Series

The Cisco uBR7200 series router is administered using the Cisco command interpreter, called the EXEC. You must boot and log in to the router before you can enter an EXEC command.

SUMMARY STEPS

1. Connect a terminal to the I/O controller console port of the Cisco uBR7200 series router and establish a terminal session.
2. Power on the Cisco uBR7200 series router. Enter no to choose the normal operating mode of the router.
3. Continue to password definition or recovery and additional configuration.

DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | Connect a terminal to the I/O controller console port of the Cisco uBR7200 series router and establish a terminal session. | You can open a Terminal application (Hyper Terminal) on a PC as follows:<br>a. Connect using: Direct to Com 1<br>b. Set bits per second: 9600<br>c. Set data bits: 8<br>d. Set parity: none<br>e. Set stop bit: 1<br>f. Set flow control: hardware |
| Step 2 | Power on the Cisco uBR7200 series router. Enter **no** to choose the normal operating mode of the router.<br><br>Example:<br>`Would you like to enter the initial dialog?[yes]:`<br>**`no`**<br>`Router>` | The user EXEC prompt appears. |
| Step 3 | Continue to password definition or recovery and additional configuration. | Refer to the remaining procedures in this chapter. |

# Setting Password Protection on the Cisco uBR7200 Series

Note For security purposes, the EXEC has two levels of access to commands: user EXEC mode and privileged EXEC mode. The commands available at the user level are a subset of those available at the privileged level.

Tip Because many privileged-level EXEC commands are used to set operating parameters, password-protect these commands to prevent unauthorized use.

SUMMARY STEPS

1. **enable secret** *password* or **enable** *password*
2. *password*

DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | At the EXEC prompt, enter one of the following two commands to set password protection:<br><br>**enable secret** *password*<br><br>or<br><br>**enable** *password*<br><br>Example:<br>`Router> enable secret cisco` | These command differ in their security level.<br>• **enable secret** *password* — Enters a very secure, encrypted password.<br>• **enable** *password* — Enters a less secure, nonencrypted password. |
| Step 2 | To gain access to privilege EXEd-level commands, enter the desired password. | |
| Step 3 | | |
| Step 4 | | |

Note
- An enable secret password can contain from 1 to 25 alphanumeric characters in uppercase and lowercase.
- An enable password can contain any number of alphanumeric characters in uppercase and lowercase.
- A number cannot be the first character.
- Spaces are valid password characters; for example, “two words” is a valid password.
- Leading spaces are ignored. Trailing spaces are recognized.
- Alphanumeric characters are recognized as uppercase or lowercase.

Passwords should be different for maximum security. If you enter the same password for both during the setup script, the system accepts it, but you receive a warning message indicating that you should enter a different password.

# Recovering Passwords on the Cisco uBR7200 Series

This section describes how to recover a lost enable or console login password and how to replace a lost enable secret password on your Cisco uBR7200 series router.

Note It is possible to recover the enable or console login password. The enable secret password is encrypted, however, and must be replaced with a new enable secret password.

## Overview of the Password Recovery Process

Following is an overview of the general steps in the password recovery procedure:

Step 1 If you can log in to the router, enter the **show version** command to determine the existing configuration register value.

Step 2 Press the **Break** key to get to the bootstrap program prompt (ROM monitor). You might need to reload the system image by power cycling the router.

Step 3 Change the configuration register so that the following functions are enabled:

- Break
- Ignore startup configuration
- Boot from Flash memory

Note The key to recovering a lost password is to set the configuration register bit 6 (0x0040) so that the startup configuration (usually in NVRAM) is ignored. This allows you to log in without using a password and to display the startup configuration passwords. Cisco recommends setting the configuration register to 0x142.

Step 4 Power cycle the router by turning power off and then back on.

Step 5 Log in to the router and enter the privileged EXEC mode.

Step 6 Enter the **show startup-config** command to display the passwords.

Step 7 Recover or replace the displayed passwords.

Step 8 Change the configuration register back to its original setting.

Note To recover a lost password if `Break` is disabled on the router, you must have physical access to the router.

## Replacing or Recovering Passwords

Complete the following steps to recover or replace a lost enable, enable secret, or console login password:

Step 1 Attach an ASCII terminal to the console port on your Cisco uBR7200 series router.

Step 2 Configure the terminal to operate at 9600 baud, 8 data bits, no parity, and 2 stop bits.

Step 3 If you can log in to the router as a nonprivileged user, enter the **show version** command to display the existing configuration register value. Note the value for later use. If you cannot log in to the router at all, continue with the next step.

Step 4 Press the **Break** key or send a Break from the console terminal.

- If Break is enabled, the router enters the ROM monitor, indicated by the ROM monitor prompt (`rommon n>`), where *n* is the number of the command line. Proceed to Step 6.
- If Break is disabled, power cycle the router (turn the router off or unplug the power cord, and then restore power). Proceed to Step 5.

Step 5 Within 60 seconds of restoring the power to the router, press the **Break** key or send a Break. This action causes the router to enter the ROM monitor and display the ROM monitor prompt (`rommon 1>`).

Step 6 To set the configuration register on a Cisco uBR7200 series router, use the configuration register utility by entering the **confreg** command at the ROM monitor prompt as follows:

```
rommon 1> confreg
```

Answer **yes** to the enable `ignore system config info?` prompt and note the current configuration register settings.

Step 7 Initialize the router by entering the **reset** command as follows:

```
rommon 2> reset
```

The router initializes, the configuration register is set to 0x142, the router boots the system image from Flash memory and enters the System Configuration dialog (setup), as follows:

```
--- System Configuration Dialog --
```

Step 8 Enter **no** in response to the System Configuration dialog prompts until the following message appears:

```
Press RETURN to get started!
```

Step 9 Press **Return.** The user EXEC prompt appears as follows:

```
Router>
```

Step 10 Enter the **enable** command to enter privileged EXEC mode.

Step 11 Enter the **show startup-config** command to display the passwords in the configuration file as follows:

```
Router# show startup-config
```

Step 12 Scan the configuration file display looking for the passwords; the enable passwords are usually near the beginning of the file, and the console login or user EXEC password is near the end. The passwords displayed will appear similar to the following:

```
enable secret 5 $1$ORPP$s9syZt4uKn3SnpuLDrhuei
enable password 23skiddoo
.
.
line con 0
 password onramp
```

Note The enable secret password is encrypted and cannot be recovered; it must be replaced. The enable and console passwords can be encrypted text or clear text.

Proceed to the next step to replace an enable secret, console login, or enable password. If there is no enable secret password, note the enable and console login passwords if they are not encrypted and proceed to Step 17.

Caution Do not perform the next step unless you have determined that you must change or replace the enable, enable secret, or console login passwords. Failure to follow the steps as presented here could cause your router configuration to be erased.

Step 13 Enter the **configure memory** command to load the startup configuration file into running memory. This action allows you to modify or replace passwords in the configuration.

```
Router# configure memory
```

Step 14 Enter the **configure terminal** command for configuration mode:

```
Router# configure terminal
```

Step 15 To change all three passwords, enter the following commands:

```
Router(config)# enable secret newpassword1
Router(config)# enable password newpassword2
Router(config)# line con 0
Router(config)# password newpassword3
```

Change only the passwords necessary for your configuration. You can remove individual passwords by using the **no** form of the previous commands. For example, entering the **no enable secret** command removes the enable secret password.

Step 16 You must configure all interfaces to *not* be administratively shut down as follows:

```
Router(config)# interface fast ethernet 0/0
Router(config)# no shutdown
```

Enter the equivalent commands for all interfaces that were originally configured. If you omit this step, all interfaces are administratively shut down and unavailable when the router is restarted.

Step 17 Use the **config-register** command to set the configuration register to the original value noted in Step 3 or Step 7.

Step 18 Press **Ctrl-Z** or type **end** to exit configuration mode:

```
Router(config)# end
```

Caution Do not perform the next step unless you have changed or replaced a password. If you have skipped Step 13 through Step 16 previously, then proceed now to Step 20. Failure to observe this sequence causes the system to erase your router configuration file.

Step 19 Enter the **copy running-config startup-config** command to save the new configuration to nonvolatile memory:

```
Router# copy running-config startup-config
```

Step 20 Enter the **reload** command to reboot the router:

```
Router# reload
```

Step 21 Log in to the router with the new or recovered passwords.

# Configuring the Cisco uBR7200 Series Using AutoInstall

This section provides information about AutoInstall, a Cisco IOS software feature that allows you to configure a new router automatically and dynamically. The AutoInstall process involves connecting a new router to a network where an existing router is preconfigured, turning on the new router, and enabling it with a configuration file that is automatically downloaded from a TFTP server.

The AutoInstall process begins any time a Cisco IOS software-based device is turned on and a valid configuration file is not found in nonvolatile random-access memory (NVRAM).

Note If you wish to configure the device manually, you should connect directly to the console port and ensure that the router is not connected to the network via any of the interface ports before you turn on the router. Note that it may take several minutes for the device to determine that AutoInstall is not connected to the network.

This section contains the following information and procedures:


- "Autoinstall Requirements" section on page 10
- "Understanding AutoInstall" section on page 11
- "Preparing for the AutoInstall Process" section on page 11
- "Performing the AutoInstall Procedure" section on page 12
- "Setting Up the TFTP Server for Autoinstall" section on page 15
- "Setting Up the BOOTP or RARP Server for Autoinstall" section on page 16
- "Connecting the New Router to the Network" section on page 16


## Autoinstall Requirements

For AutoInstall to work properly, the following conditions must be met:

- Routers must be attached physically to the network using one or more of the following interface types:
  - Ethernet
  - Token Ring
  - FDDI
  - Serial with High-Level Data Link Control (HDLC) encapsulation
  - Serial with Frame Relay encapsulation

Note HDLC is the default serial encapsulation. If the AutoInstall process fails over HDLC, the Cisco IOS software automatically configures Frame Relay encapsulation.

Note Of Token Ring interfaces, only those that set ring speed with physical jumpers support AutoInstall. AutoInstall does not work with Token Ring interfaces for which the ring speed must be set with software configuration commands. If the ring speed is not set, the interface is set to shutdown mode.

- A TCP/IP host on your network must be preconfigured to provide the required configuration files.
- The TCP/IP host can exist anywhere on the network as long as the following conditions are maintained:
  - The host must be on the LAN or WAN side of the router's line card connection to the WAN.
  - The User Datagram Protocol (UDP) broadcasts to and from the router.
  - The TCP/IP host is enabled.

This functionality is coordinated by your system administrator at the site where the TCP/IP host is located. You should not use AutoInstall unless the required files are available on the TCP/IP host.

# Understanding AutoInstall

Once the requirements for using AutoInstall are met, the dynamic configuration of the new router occurs as follows:

1. The new router acquires its IP address. Depending on the interface connection between the two routers and/or access servers, the new router's IP address is dynamically resolved by either SLARP requests or BOOTP or RARP requests.
2. The new router resolves its name through network-confg, cisconet.cfg, or DNS.
3. The new router automatically requests and downloads its configuration file from a TFTP server.
4. If a host name is not resolved, the new router attempts to load router-confg or ciscortr.cfg.

# Preparing for the AutoInstall Process

Complete the following steps to prepare your Cisco uBR7200 series CMTS router for the AutoInstall process:

Step 1 Attach the appropriate synchronous serial cable to the synchronous serial interface 0 on the router.

Step 2 Turn the power switch on each power supply to the ON (|) position. This action turns on power to the router.

The router loads the operating system image from Flash memory; this process can take several minutes. If the remote end of the WAN connection is connected and properly configured, the AutoInstall process begins.

Step 3 When the AutoInstall process is completed, use the **copy running-config startup-config** command to write the configuration data to the router's nonvolatile random-access memory (NVRAM):

```
Router# copy running-config startup-config
```

Completing this step saves the configuration settings that the AutoInstall process created to NVRAM. If you fail to do this, your configuration will be lost the next time you reload the router.

Step 4 Choose your preferred method to verify the required file configurations for the AutoInstall Facility:

| | Task | Description |
|---|---|---|
| a. | Verify that the configuration file is on the TFTP server. | *Complete this task first (required).* Verify that a configuration file for the new router resides on a TFTP server. This file can contain the full or minimum-required configuration for the administrator to Telnet into the new router (for configuration using Autoinstall).<br>Note In addition, complete one of the following two tasks. |
| b. | Verify that a file named network-confg also resides on the TFTP server. | *Complete this task, or task c.* In this task, verify that the network-confg file on the TFTP server has an Internet Protocol (IP) host name entry for the new router. The TFTP server must be reachable from the new router. |
| c. | Add IP-address-to-host name mapping to a DNS database file. | *Complete this task, or task b.* In this task, add an IP address-to-host name mapping for the new router to a Domain Name System (DNS) database file on the TFTP server. |

Step 5 If the existing router is to help install the new router automatically via an HDLC-encapsulated serial interface using Serial Line Address Resolution Protocol (SLARP), that interface must be configured with an IP address whose host portion has the value 1 or 2. (AutoInstall over Frame Relay does not have this address constraint.) Subnet masks of any size are supported.

Step 6 If the existing router is to help install the new router automatically using a Frame Relay-encapsulated serial interface, that interface must be configured with the following:

- An IP helper address pointing to the TFTP server. In the following example, 171.69.2.75 is the address of the TFTP server:

  ip helper 171.69.2.75

- A Frame Relay map pointing back to the new router. In the following example, 172.21.177.100 is the IP address of the new router's serial interface, and 100 is the PVC identifier:

  frame-relay map ip 172.21.177.100 100 dlci

Step 7 If the existing router is to help install the new router automatically via an Ethernet, Token Ring, or FDDI interface using BOOTP or Reverse Address Resolution Protocol (RARP), then a BOOTP or RARP server also must be set up to map the new router's Media Access Control (MAC) address to its IP address.

Step 8 IP helper addresses might need to be configured to forward the TFTP and DNS broadcast requests from the new router to the host that is providing those services.

# Performing the AutoInstall Procedure

This procedure provides the steps to configure your Cisco uBR7200 series router using AutoInstall.

Note For a detailed description of the processes involved with AutoInstall, refer to the chapter titled "Using Configuration Tools" in the *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.1 on Cisco.com.

To dynamically configure a new router using AutoInstall, complete the following steps. Steps 1, 2, and 3 are completed by the central administrator. Step 4 is completed by the person at the remote site.

Step 1 Modify the existing router's configuration to support the AutoInstall procedure.

Step 2 Set up the TFTP server to support the AutoInstall procedure.

Step 3 Set up the BOOTP or RARP server if needed. A BOOTP or RARP server is required for AutoInstall using an Ethernet, Token Ring, FDDI, or Frame Relay-encapsulated serial interface. With a Frame Relay-encapsulated serial interface, the existing router acts as the BOOTP server. A BOOTP or RARP server is not required for AutoInstall using an HDLC-encapsulated serial interface.

Step 4 Connect the new router to the network.

## Configuring an Interface to Allow Use of AutoInstall

You can use AutoInstall through any of the following types of interfaces:

- Using an HDLC-Encapsulated Serial Interface Connection (the default configuration for a serial line)
- Using an Ethernet, Token Ring, or FDDI Interface Connection
- Using a Frame Relay-Encapsulated Serial Interface Connection

### Using an HDLC-Encapsulated Serial Interface Connection

To set up AutoInstall via a serial line with HDLC encapsulation (the default), you must configure the existing router. Use the following commands, beginning in global configuration mode:

| | Command | Purpose |
|---|---|---|
| Step 1 | **interface serial** *interface-number* | Configures the serial interface that connects to the new router with HDLC encapsulation (the default), and enters interface configuration mode for the specified interface number. |
| Step 2 | **ip address** *address mask* | Enters an IP address for the interface. The host portion of the address must have a value of 1 or 2. (AutoInstall over Frame Relay does not have this address constraint.) |
| Step 3 | **ip helper-address** *address* | Configures a helper address for the serial interface to forward broadcasts associated with the TFTP, BOOTP, and DNS requests. |
| Step 4 | **clock rate bps** | (Optional) Configures a DCE clock rate for the serial line, unless an external clock is being used. This step is needed only for DCE appliques. |
| Step 5 | Ctrl-Z | Exits configuration mode. |
| Step 6 | **copy running-config startup-config** | Saves the configuration file to your startup configuration. On most platforms, this step saves the configuration to NVRAM. On the Cisco7000 family, this step saves the configuration to the location specified by the CONFIG_FILE environment variable. |

In the following example, the existing router's configuration file contains the commands needed to configure the router for AutoInstall on a serial line using HDLC encapsulation:

```
Router# more system:startup-config
. . .
interface serial 0
 ip address 172.31.10.1 255.255.255.0
 ip helper-address 172.31.20.5
. . .
```

### Using an Ethernet, Token Ring, or FDDI Interface Connection

To set up AutoInstall using an Ethernet, Token Ring, or FDDI interface, you must modify the configuration of the existing router. Use the following commands, beginning in global configuration mode:

| | Command | Purpose |
|---|---|---|
| Step 1 | **interface** {**ethernet** \| **tokenring** \| **fddi**} *interface-number* | Enters interface configuration mode for the specified LAN interface. |
| Step 2 | **ip address** *address mask* | Specifies an IP address for the interface. |
| Step 3 | **ip helper-address** *address* | (Optional) Configures a helper address to forward broadcasts associated with the TFTP, BOOTP, and DNS requests. |
| Step 4 | Ctrl-Z | Exits configuration mode. |
| Step 5 | **copy running-config startup-config** | Saves the configuration file to your startup configuration. On most platforms, this step saves the configuration to NVRAM. On the Cisco7000 family, this step saves the configuration to the location specified by the CONFIG_FILE environment variable. |

Typically, the LAN interface and IP address are already configured on the existing router. You might need to configure an IP helper address if the TFTP server is not on the same network as the new router.

In the following example, the existing router's configuration file contains the commands needed to configure the router for AutoInstall on an Ethernet interface:

```
Router# more system:startup-config
. . .
interface Ethernet 0
ip address 172.31.10.1 255.255.255.0
ip helper-address 172.31.20.5
. . .
```

### Using a Frame Relay-Encapsulated Serial Interface Connection

To set up AutoInstall via a serial line with Frame Relay encapsulation, you must configure the existing router. Use the following commands beginning in global configuration mode:

| | Command | Purpose |
|---|---|---|
| Step 1 | **interface serial 0** | Configures the serial interface that connects to the new router, and enters interface configuration mode. |
| Step 2 | **encapsulation frame-relay** | Configures Frame Relay encapsulation on the interface that connects to the new router. |
| Step 3 | **frame-relay map ip** *ip-address dlci*<br>or<br>**frame-relay interface-dlci** *dlci option* [**protocol ip** *ip-address*] | Creates a Frame Relay map pointing back to the new router.<br>or<br>For point-to-point subinterfaces, assigns a data link connection identifier (DLCI) to the interface that connects to the new router, and provides the IP address of the serial port on the new router. |
| Step 4 | **ip address** *address mask* | Specifies an IP address for the interface. This step sets the IP address of the existing router. |
| Step 5 | **ip helper-address** *address* | Configures a helper address for the TFTP server. |
| Step 6 | _(_IREFOBJ:1006127_)<br>_clock rate bps | (Optional) Configures a DCE clock rate for the serial line, unless an external clock is being used. This step is needed only for DCE appliques. |
| Step 7 | Ctrl-Z | Exits configuration mode. |
| Step 8 | **copy running-config startup-config** | Saves the configuration file to your startup configuration.<br>Note On most platforms, this step saves the configuration to NVRAM. On the Cisco 7000 family, this step saves the configuration to the location specified by the CONFIG_FILE environment variable. |

You must use a DTE interface on the new router because the network always provides the clock signal.

In the following example, the existing router's configuration file contains the commands needed to configure the router for Frame Relay AutoInstall on a serial line:

```
Router# more system:startup-config
. . .
interface serial 0
ip address 172.31.20.20 255.255.255.0
encapsulation frame-relay
frame-relay map ip 172.31.10.1 255.255.255.0 48
ip helper-address 172.31.20.5
. . .
```

# Setting Up the TFTP Server for Autoinstall

For AutoInstall to work correctly, the new router must be able to resolve its host name and then download a name-confg or a name.cfg file from a TFTP server. The new router can resolve its host name by using a network-confg or a cisconet.cfg file downloaded from a TFTP server or by using the DNS.

To set up a TFTP server to support AutoInstall, perform the following steps:

Step 1 Enable TFTP on a server. For information on this process, consult your host vendor's TFTP server documentation and RFCs 906 and 783.

Step 2 If you want to use a network-confg or cisconet.cfg file to resolve the new router's name, create the network-confg or cisconet.cfg file containing an IP address-to-host name mapping for the new router. Enter the ip host command into the TFTP config file, not into the router. The IP address must match the IP address that is to be dynamically obtained by the new router.

If you want to use DNS to resolve the new router's name, create an address-to-name mapping entry for the new router in the DNS database. The IP address must match the IP address that is to be dynamically obtained by the new router. For more information on this step, contact your DNS administrator or refer to RFCs 1101 and 1183.

Step 3 Create the name-confg or name.cfg file, which should reside in the tftpboot directory on the TFTP server. The name part of name-confg or name.cfg filename must match the host name you assigned for the new router in the previous step. Enter configuration commands for the new router into this file.

The name-confg or the name.cfg file can contain either the new router's full configuration or a minimal configuration.

The minimal configuration file is a virtual terminal password and an enable password. It allows an administrator to Telnet into the new router to configure it. If you are using BOOTP or RARP to resolve the address of the new router, the minimal configuration file must also include the IP address to be obtained dynamically using BOOTP or RARP.

You can use the **copy running-config tftp** command to help you generate the configuration file that you later download during the AutoInstall process.

Note The existing router might need to forward TFTP requests and response packets if the TFTP server is not on the same network segment as the new router. When you modified the existing router's configuration, you specified an IP helper address for this purpose.

You can save a minimal configuration under a generic newrouter-confg file. Use the **ip host** command in the network-confg or cisconet.cfg file to specify newrouter as the host name with the address you will be dynamically resolving. The new router should then resolve its IP address, host name, and minimal configuration automatically.

Use Telnet to connect to the new router from the existing router and use the **setup** command facility to configure the rest of the interfaces. For example, the line in the network-confg or cisconet.cfg file could be similar to the following:

```
ip host newrouter 131.108.170.1
```

The following host configuration file contains the minimal set of commands needed for AutoInstall using SLARP or BOOTP:

```
enable-password letmein
!
line vty 0
password letmein
!
end
```

The preceding example shows a minimal configuration for connecting from a router one hop away. From this configuration, use the setup facility to configure the rest of the interfaces. If the router is more than one hop away, you also must include routing information in the minimal configuration.

The following minimal network configuration file maps the new router's IP address, 131.108.10.2, to the host name newrouter. The new router's address was learned via SLARP and is based on the existing router's IP address of 131.108.10.1.

```
ip host newrouter 131.108.10.2
```

# Setting Up the BOOTP or RARP Server for Autoinstall

If the new router is connected to the existing router using an Ethernet, Token Ring, or FDDI interface, you must configure a BOOTP or RARP server to map the new router's MAC address to its IP address. If the new router is connected to the existing router using a serial line with HDLC encapsulation, or if you are configuring AutoInstall over Frame Relay, the tasks in this section are not required.

To configure a BOOTP or RARP server, use one of the following commands:

| Command | Purpose |
|---|---|
| Refer to your host vendor's documentation and to RFCs 951 and 1395 | If BOOTP is to be used to resolve the new router's IP address, configure your BOOTP server. |
| Refer to your host vendor's documentation and to RFC 903 | If RARP is to be used to resolve the new router's IP address, configure your RARP server. |

Note If the RARP server is not on the same subnet as the new router, use the **ip rarp-server** command to configure the existing router to act as a RARP server. For more information, see the "Configuring a Router as a RARP Server" section.

The following host configuration file contains the minimum set of commands needed for AutoInstall using RARP. It includes the IP address that will be obtained dynamically via BOOTP or RARP during the AutoInstall process. When RARP is used, this extra information is needed to specify the proper netmask for the interface.

```
interface ethernet 0
ip address 131.108.10.2 255.255.255.0
enable-password letmein
!
line vty 0
password letmein
!
end
```

# Connecting the New Router to the Network

Connect the new router to the network using either an HDLC-encapsulated or Frame Relay-encapsulated serial interface or an Ethernet, Token Ring, or FDDI interface. After the router successfully resolves its host name, newrouter sends a TFTP broadcast requesting the file name-confg or name.cfg. The router name must be in all lowercase, even if the true host name is not. The file is downloaded to the new router, where the configuration commands take effect immediately. If the configuration file is complete, the new router should be fully operational.

To save the complete configuration to NVRAM, use the following commands in privileged EXEC mode:

| | Command | Purpose |
|---|---|---|
| Step 1 | **enable password** | Enters privileged mode on the new router. |
| Step 2 | **copy running-config startup-config** | Saves the information from the name-config file into your startup configuration. On most platforms, this step saves the configuration to NVRAM. On the Cisco 7000 family, this step saves the configuration to the location specified by the CONFIG_FILE environment variable. |

Caution Verify that the existing and new routers (or access servers) are connected before entering the **copy running-config startup-config** EXEC command to save configuration changes. Use the **ping** EXEC command to verify connectivity. If an incorrect configuration file is downloaded, the new router will load NVRAM configuration information before it can enter AutoInstall mode.

If the configuration file is a minimal configuration file, the new router comes up, but with only one interface operational. Use the following commands to connect to the new router and configure it:

| | Command | Purpose |
|---|---|---|
| Step 1 | **telnet existing** | Establishes a Telnet connection to the existing router. |
| Step 2 | **telnet** *newrouter* | From the existing router, establishes a Telnet connection to the new router. |
| Step 3 | **enable** *password* | Enters privileged EXEC mode. |
| Step 4 | **setup** | Enters setup mode to configure the new router. |

# Configuring the Cisco uBR7200 Series Using the Setup Facility

## Introduction to the Setup Facility

The Cisco uBR7200 series Setup facility (also called the System Configuration dialog) is a useful and efficient tool for configuring your CMTS. The Cable Interface Setup Facility is an alternative mechanism to enable or configure Cisco uBR7200 series parameters. The Setup facility supports automated configuration of upstream parameters.

In earlier releases, upstream ports were put in a default shut-down state after the Setup facility was run. You had to use the CLI to configure a fixed frequency or create a spectrum group, assign an interface to it, and enable each upstream port on a cable interface line card. The Setup facility now supports configuring and enabling upstream parameters.

The Setup facility supports the following functions so that cable interfaces and cable interface line cards are fully operational after initial setup:

- Cable-specific commands
- Upstream frequency definition

For each cable interface, the following information is mandatory:

```
Per upstream:
        cable upstream n frequency f
        no cable upstream n shutdown
```

Options include definition of the following information:

- DHCP server address.
- Options are also provided to set downstream frequency for the upconverter per interface.

If you do not plan to use AutoInstall, do not connect the router's WAN or LAN cable to the channel service unit (CSU) and data service unit (DSU). If the WAN or LAN cable is connected to the CSU and DSU and the router does not have a configuration stored in NVRAM, the router attempts to run AutoInstall at startup.

Tip The router might take several minutes to determine that AutoInstall is not set up to a remote TCP/IP host.

When the router determines that AutoInstall is not configured, it defaults to the Setup facility. If the LAN or WAN cable is not connected, the router boots from Flash memory and automatically runs the Setup facility.

Note You can run the Setup facility when the enable prompt (#) is displayed, by entering the **setup** command in privileged EXEC mode.

# Configuring Global Parameters with the Setup Facility

When you first start the program, configure the global parameters to control system-wide settings:

Step 1 Connect a console terminal to the console port on the I/O controller, and then boot the router.

Step 2 After booting from Flash memory, the following information appears after about 30 seconds. When you see this information, you have successfully booted your router:

```
           Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (UBR7200-IK1S-M), Version 12.1(10)EC
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 24-Nov-01 12:59 by yiyan
Image text-base: 0x60008950, data-base: 0x61478000

Compliance with U.S. Export Laws and Regulations - Encryption

This product performs encryption and is regulated for export
by the U.S. Government.

This product is not authorized for use by persons located
outside the United States and Canada that do not have prior
approval from Cisco Systems, Inc. or the U.S. Government.

This product may not be exported outside the U.S. and Canada
either by physical or electronic means without PRIOR approval
of Cisco Systems, Inc. or the U.S. Government.

Persons outside the U.S. and Canada may not re-export, resell,
or transfer this product by either physical or electronic means
without  prior approval of Cisco Systems, Inc. or the U.S.
Government.

Cisco uBR7246VXR (NPE300) processor (revision D) with 253952K/40960K bytes
of memory.
Processor board ID SAB0433019F
R7000 CPU at 262Mhz, Implementation 39, Rev 2.1, 256KB L2, 2048KB L3 Cache
6 slot VXR midplane, Version 2.0
```

```
Last reset from power-on
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
4 Serial network interface(s)
4 Cable Modem network interface(s)
125K bytes of non-volatile configuration memory.

125440K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
4096K bytes of Flash internal SIMM (Sector size 256K).
cable submgmt default active

Press RETURN to get started!
```

Note The first two sections of the configuration script, the banner and the installed hardware, appear only at initial system startup. On subsequent uses of the **Setup facility**, the script begins with the following prompt.

```
        --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
```

Step 3 When asked if you want to continue with the System Configuration dialog and enter basic management setup (displays the current interface summary), enter **yes** or press **Return**:

```
Continue with configuration dialog? [yes/no]: yes
.
.
.
Would you like to enter basic management setup? [yes/no]: yes
```

The interface summary appears, showing the state of configured and unconfigured interfaces.

Step 4 Choose which protocols to support on your interfaces. For IP-only installations, you can accept the default values for most of the questions. A typical configuration using IP follows and continues through Step 7:

```
Configuring global parameters:

  Enter host name [Router]: router
```

Step 5 Enter the enable secret password, the enable password, and the virtual terminal password:

```
The enable secret password is a one-way cryptographic secret
password used instead of the enable password when it exists.

  Enter enable secret: ******

The enable password is used when there is no enable secret
password and when using older software and some boot images.

  Enter enable password: ******

Enter virtual terminal password: ******
```

Step 6 The Simple Network Management Protocol (SNMP) is the most widely supported open standard for network management. SNMP provides a means to access and set configuration and run-time parameters of routers and communication servers. SNMP also defines a set of functions that can be used to monitor and control network elements.

Enter **yes** to accept SNMP management; enter **no** to refuse it:

```
Configure SNMP Network Management? [no]:
    Community string [public]:
```

Step 7 In all cases, you will use IP routing. When you are using IP routing, select an interior routing protocol. You can specify one of only two interior routing protocols to operate on your system using the Setup facility, either Interior Gateway Routing Protocol (IGRP) or Routing Information Protocol (RIP).

To configure IP routing, enter **yes** (the default) or press **Return**, and then select an interior routing protocol:

```
  Configure IP? [yes]:
    Configure IGRP routing? [yes]:
      Your IGRP autonomous system number [1]: 15
```

Step 8 Configure your line card interface parameters. The following example shows how an 8-port Ethernet line card is installed in line card slot 3. The Setup facility determines the status of all interfaces.

To configure each active interface port for IP, enter **yes** (the default) or press **Return**. For all inactive ports, the default is **no**. You can press **Return** to accept the default.

```
Configuring interface Ethernet 1/0:
  Is this interface in use? [yes]:
  Configure IP on this interface? [yes]:
    IP address for this interface [19.2.22.4]:
    Number of bits in subnet field [8]:
    Class A network is 19.0.0.0, 8 subnet bits; mask is /16

Configuring interface Ethernet1/1:
  Is this interface in use? [no]:

Configuring interface Ethernet1/2:
Is this interface in use? [no]:

Configuring interface Ethernet1/3:
  Is this interface in use? [no]:

Configuring interface Ethernet1/4:
  Is this interface in use? [no]:

Configuring interface Ethernet1/5:
  Is this interface in use? [no]:

Configuring interface Ethernet1/6:
  Is this interface in use? [no]:

Configuring interface Ethernet1/7:
  Is this interface in use? [no]:
```

Step 9 Configure your cable interface. The following example shows a Cisco uBR7200 series router with cable interface. The Setup facility, for the most part, determines the status of all interfaces.

To configure each active interface port, enter **yes** (the default) or press **Return**. For all inactive ports, the default is **no**. You can press **Return** to accept the default.

```
Configuring interface cable 5/0:
  Is this interface in use? [yes]:
  Configure this interface? [yes]:
  IP address for this interface [19.2.22.5]:
  Number of bits in subnet field [8]:
  Class A network is 19.0.0.0, 8 subnet bits; mask is /16

Configuring interface cable 1/1:
```

```
  Is this interface in use? [yes]:
  Configure this interface? [yes]:
  IP address for this interface [19.2.22.6]:
  Number of bits in subnet field [8]:
  Class A network is 19.0.0.0, 8 subnet bits; mask is /16
```

The configuration program displays the newly created command interface script:

```
The following command script was created:

hostname router
enable secret 5 $1$f0fc$A38P/KN/9yD3sEKSt6hKQ/
enable password betty
line vty 0 4
password wilma
snmp-server community public
!
ip routing
!
interface cable 5/0
ip address 19.2.22.5 255.255.0.0

router igrp 15
network 19.0.0.0
!
end
```

Step 10 When asked if you want to use this configuration, enter **yes** or press **Return.**

```
Use this configuration? [yes/no]: yes
```

Step 11 Save the configuration to NVRAM:

```
Router# copy running-config startup-config
```

Note You must always manually save the configuration settings to NVRAM whenever they are modified.

# Configuring Upstream Frequencies with the Setup Facility

Upstream parameters must be configured manually. After the **Setup facility** is run, upstream ports have a default state of "shutdown." You have two methods to configure upstream channel frequencies:

- Configure a fixed frequency between 5 to 42 MHz for North American channel plans, and enable the upstream port.
- Create a global spectrum group, assign the interface to it, and enable the upstream port.

The cable interface card receiver accepts time-division multiplexed burst transmissions from cable interfaces (or CMs in set-top boxes), which are DOCSIS-based. The upstream port becomes "up" when it is assigned an upstream frequency and is configured to be administratively up.

The upstream port is frequency-agile. The frequency can change while the interface is up and carrying traffic, if you define spectrum groups per the example provided.

## Configuring Individual Upstream Modulation Profiles

You can define individual modulation profiles. A modulation profile consists of a table of physical layer characteristics for the different types of upstream bursts such as initial maintenance, long grant, request data, request, short grant, and station maintenance.

Note Only qualified personnel should define upstream modulation profiles.

Complete these steps to activate upstream interfaces:

Step 1 After the Setup facility has initially configured noncable interfaces on the Cisco uBR7200 series router, enter the **enable** command and your password (privileged EXEC).

Step 2 Enter the **configure terminal** command to get into global configuration mode.

Step 3 In global configuration mode, configure modulation profiles and spectrum groups for your Cisco uBR7200 series router using the **cable modulation-profile** and **cable spectrum-group** commands.

Step 4 In cable interface configuration mode, configure various characteristics for the interface in question, using the **cable upstream** commands.

Note Refer to Chapter 2, "Configuring the Cable Modem Termination System for the First Time," for further information.

# Configuring Interfaces with the Setup Facility

Follow the procedure in this section to configure WAN or LAN interfaces. To configure interface parameters, have your interface network addresses and subnet mask information ready.

## Configuring Ethernet Interfaces

Step 1 In the following example, the system is being configured for an Ethernet LAN using IP. Respond to the prompts as follows, using your own addresses and mask at the setup prompts:

```
Configuring interface parameters:
Configuring interface Ethernet0/0:
Is this interface in use? [no]: yes
Configure IP on this interface? [no]: yes
IP address for this interface: 1.1.1.10
Number of bits in subnet field [0]:
Class A network is 1.0.0.0, 0 subnet bits; mask is 255.0.0.0
```

Step 2 Do not enable Internetwork Package Exchange (IPX) on this interface; IPX is not supported on the Cisco uBR7200 series universal broadband router:

```
Configure IPX on this interface? [no]: no
```

Step 3 If additional Ethernet interfaces are available in your system, enter their configurations when you are prompted.

Step 4 Save the configuration to NVRAM:

```
Router# copy running-config startup-config
```

Note You must always manually save the configuration settings to NVRAM whenever they are modified.

## Configuring Synchronous Serial Interfaces

The synchronous serial interfaces are configured to allow connection to WANs through a CSU/DSU. Complete the following steps to configure the serial ports:

Step 1 To configure serial port 0 enter yes:

```
Configuring interface Serial0/0:
  Is this interface in use? [no]: yes
```

Step 2 Determine which protocols you want on the synchronous serial interface and enter the appropriate responses:

```
Configure IP unnumbered on this interface? [no]:
    IP address for this interface: 10.1.1.20
Number of bits in subnet field [0]:
    Class A network is 10.0.0.0, 0 subnet bits; mask is 255.0.0.0
```

Step 3 If additional synchronous serial interfaces are available in your system, enter their configurations when you are prompted.

Step 4 Save the configuration to NVRAM:

```
Router# copy running-config startup-config
```

Note You must always manually save the configuration settings to NVRAM whenever they are modified.

The following sample display includes a continuous listing of all interface configuration parameters selected for Ethernet and synchronous serial interfaces. These parameters are shown in the order in which they appear on your console terminal.

Tip Only one Ethernet and one synchronous serial interface are configured for this example.

```
Configuring interface parameters:

Configuring interface Ethernet0/0:
  Is this interface in use? [no]: yes

  Configure IP on this interface? [no]: yes

    IP address for this interface: 10.1.1.10

    Number of bits in subnet field [0]:
    Class A network is 10.0.0.0, 0 subnet bits; mask is 255.0.0.0
  Configure IPX on this interface? [no]:
  Configure AppleTalk on this interface? [no]: no

Configuring interface Serial0/0:
  Is this interface in use? [no]: yes

  Configure IP on this interface? [no]: yes

  Configure IP unnumbered on this interface? [no]:
    IP address for this interface: 10.1.1.20

    Number of bits in subnet field [0]:
    Class A network is 10.0.0.0, 0 subnet bits; mask is 255.0.0.0
  Configure IPX on this interface? [no]:
  Configure AppleTalk on this interface? [no]:
```

```
The following configuration command script was created:

hostname Router
enable secret 5 $1$u8z3$PMYY8em./8sszhzk78p/Y0
enable password wilma
line vty 0 4
password s
snmp-server community public
!
ip routing
no vines routing
no ipx routing
no appletalk routing
no apollo routing
no decnet routing
no xns routing
no clns routing
no bridge 1


! Turn off IPX to prevent network conflicts.
interface Ethernet0/0
no ipx network
interface Ethernet0/1
no ipx network
!
interface Ethernet0/0
ip address 1.1.1.10 255.0.0.0
no mop enabled
!
interface serial0/0
ip address 1.1.1.20 255.0.0.0
ip route-cache cbus
no keepalive
!
!
router igrp 15
network 1.0.0.0
!
end

Use this configuration? [yes/no]: yes

[OK]
Use the enabled mode `configure' command to modify this configuration.

Press RETURN to get started!
```

Your Cisco uBR7200 series router is now minimally configured and is ready to use. Use the **setup** command in provileged EXEC mode if you want to modify the parameters after the initial configuration. To perform more complex configurations, use the **configure** privileged EXEC command in global configuration mode.

## Setup Facility Examples

In the following example, the upstream parameters for a cable interface line card in slot 5 are configured and enabled. Press Return to accept the default.

```
Do you want to configure Cable 5/0 interface? [no]: yes
Downstream setting frequency: 531000000
For cable upstream [0]
Shut down this upstream? [yes/no]: no
Frequency: 33808000
Would you like to configure the DHCP server? [yes/no]: yes
```

```
IP address for the DHCP server [X.X.X.X]: 10.0.0.2
Configure IP on this interface? [yes]:
IP address for this interface [10.20.133.65]:
Subnet mask for this interface [255.0.0.0]: 255.255.255.248
Class A network is 10.0.0.0, 29 subnet bits; mask is /29
In this example, the input above generates the following command interface script:
interface Cable 5/0
no shutdown
cable downstream frequency 531000000
no shutdown
cable downstream modulation 64qam
cable downstream annex B
cable downstream interleave-depth 32
no cable upstream 0 shutdown
cable upstream 0 frequency 33808000
cable helper-address 10.0.0.2
ip address 10.20.133.65 255.255.255.248
```

Note Cable modems or set-top boxes with integrated cable modems are brought online when the utility is run.

Note For Dynamic Host Configuration Protocol (DHCP)/time of day (TOD)/Trivial File Transfer Protocol (TFTP), a static route must exist to the host.

# Configuring the Cable Interface with the Extended Setup Facility

The Setup facility creates an initial configuration. The basic management setup configures only enough connectivity for management of the system. The Extended setup facility prompts you to configure each interface on the system.

To invoke the configuration facility, use the following command:

```
Router# setup
```

The following is the System Configuration dialog:

```
Continue with configuration dialog? [yes/no]: yes
```

## Identifying the Cable Interface Line Card

### Identifying Cable Modem Line Cards

The following Cisco cable interfaces can be installed in a Cisco CMTS:

- The Cisco uBR7200 series router supports one downstream modulator and one upstream demodulator.
  - The Cisco uBR7200 series router supports the following defaults: QAM-256 at 40 MBps downstream, and QAM-16 at 5 Mbps upstream.
  - The card supports upstream channel widths of 200 kHz, 400 kHz, 800 kHz, 1.6 MHz, and 3.2 MHz.
  - The card outputs +42 dBmV and +/- 2 dBmV.
  - The downstream modulator has both an RF output, using the integrated upconverter, and an intermediate frequency (IF) output, which must be connected to an external upconverter.

## Identifying Cable Modem Line Card Slots

On the Cisco uBR7200 series router, the cable interface line card is fixed and is always slot 1. To display information about a specific cable interface slot's downstream channel, use the **show interfaces cable** command with the CM card's slot number and downstream port number in the following format:

**show interfaces cable** *slot/downstream-port* [**downstream**]

Use the slot number and downstream port number to display information about a downstream interface. You can abbreviate the command to **sh int c**. The following example shows the display for upstream channel port 0 on a Cisco uBR7200 series router:

```
Router# sh int c 5/0
```

To display information about a specific cable interface slot's upstream channel, use the **show interfaces cable** command. Include these CM card parameters:

- Slot number
- Downstream port number
- Upstream port number

Use this format:

**show interfaces cable** *slot/downstream-port* [**upstream**] *upstream-port*

Use the slot number, downstream port number, and upstream port number to display information about an upstream interface. You can abbreviate the command to **sh int c**.

The following example shows the display for upstream channel port 0 in cable interface slot 3 of a Cisco uBR7200 series router that is turned up:

```
Router# sh int c3/0 upstream
```

# Configuring Global Parameters in Extended Setup

Step 1 Access the host by responding to the following prompt:

```
Enter host name [cmts]:
```

The enable secret password is used to protect access to privileged EXEC and configuration modes. This password, after entered, becomes encrypted in the configuration.

Step 2 Respond to this prompt:

```
Enter enable secret [Use current secret]: aa
```

Next, the enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images.

Step 3 Respond to this prompt:

```
Enter enable password [rHoz]: bb
```

Next, use the virtual terminal password to protect access to the router over a network interface.

Step 4 Respond to this prompt:

```
Enter virtual terminal password [cc]: cc
```

The following system information appears.

```
Configure SNMP Network Management? [no]:
```

```
Configure IP? [yes]:
Configure IGRP routing? [yes]:
Your IGRP autonomous system number [1]:
Configure CLNS? [no]:
Configuring interface parameters:
Do you want to configure FastEthernet0/0  interface? [yes]:
Use the 100 Base-TX (RJ-45) connector? [yes]:
Operate in full-duplex mode? [no]:
Configure IP on this interface? [yes]: no
Do you want to configure Ethernet1/0  interface? [yes]: n
Do you want to configure Cable5/0  interface? [yes]:
Downstream setting frequency  : 531000000
For cable upstream [0]
Shut down this upstream ? [yes/no]: no
Frequency  : 33808000
Would you like to configure the DHCP server ? [yes/no]: yes
IP address for the DHCP server
[X.X.X.X]: 10.0.0.2
Configure IP on this interface? [no]: yes
IP address for this interface: 10.20.133.65
Subnet mask for this interface [255.0.0.0] : 255.255.255.248
Class A network is 10.0.0.0, 29 subnet bits; mask is /29
```

The following configuration command script is created:

```
interface cable5/0
ip address 10.20.133.65 255.255.255.248
no ip mroute-cache
no keepalive
cable insertion-interval 500
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream frequency 531000000
cable upstream 0 frequency 33808000
cable upstream 0 power-level 0
no cable upstream 0 shutdown
cable helper-address 10.0.0.2
```

Note For modems to acquire an IP address, they must have direct access to DHCP, TFTP, or ToD servers, or have a static route set.

# Configuring the Cisco uBR7200 Series Manually Using Configuration Mode

You can configure the Cisco uBR7200 series router manually if you prefer not to use the Setup facility or AutoInstall. Complete the following steps:

Step 1 Connect a console terminal to the console port on the I/O controller.

Step 2 When asked if you want to enter the initial dialog, respond **no** to go into the normal operating mode of the router:

```
Would you like to enter the initial dialog? [yes]: no
```

Step 3 After a few seconds, the user EXEC prompt (`Router>`) appears. Type **enable** to enter enable mode (configuration changes can be made only in enable mode):

```
Router> enable
```

The prompt changes to the enable mode (also called privileged EXEC) prompt:

```
Router#
```

Step 4 Enter the **configure terminal** command (**conf t**)at the enable prompt to enter configuration mode from the terminal:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Tip To see a list of the configuration commands available to you, enter **?** at the prompt or type **help** while in configuration mode.

Step 5 At the `Router(config)#` prompt, enter the **interface** *type slot/port* command to enter the interface configuration mode:

```
Router(config)# interface cable slot/port
Router(config-if)#
```

Step 6 Set the downstream center frequency to reflect the digital carrier frequency of the downstream RF carrier (the channel) for the downstream port:

```
Router(config-int)# cable downstream frequency down-freq-hz
```

Note This command has no effect on the external upconverter. It is informational only.

Step 7 Activate the downstream port on the cable interface line card to support digital data transmission over the hybrid fiber-coaxial network:

```
Router(config-int)# no shutdown
```

Step 8 Enter the fixed center frequency in Hz for your downstream RF carrier and the port number:

```
Router(config-int)# cable upstream port frequency up-freq-hz
```

Note Be sure not to select an upstream frequency that interferes with that used for any other upstream application in your cable plant.

Step 9 Repeat Step 8 for each upstream port on the cable interface line card.

Step 10 Activate the upstream port:

```
Router(config-int)# no cable upstream port shutdown
```

Step 11 Repeat Step 10 to activate each port used on your cable interface line card.

Step 12 Exit to return to the configuration mode:

```
Router(config-if)# exit
Router(config)#
```

Step 13 Enter the next interface to configure, following Step 6 through Step 12, or type **exit** to return to enable mode.

```
Router(config)# exit
Router#
%SYS-5-CONFIG_I: Configured from console by console#
```

Step 14 Save the configuration to NVRAM:

```
Router# copy running-config startup-config
```

# Saving Your Configuration Settings

To store the configuration or changes to your startup configuration in NVRAM, enter the **copy running-config startup-config** command at the `Router#` prompt:

```
Router# copy running-config startup-config
```

This command saves the configuration settings you set using configuration mode, the Setup facility, or AutoInstall.

Tip If you do not save your settings, your configuration will be lost the next time you reload the router.

# Reviewing Your Settings and Configurations

You can check your settings and review any changes to your configuration using various software commands.

- To view information specific to the hardware and cable interface configuration on your Cisco uBR7200 series router, use **show** commands.
  - Use the following command to verify the downstream center frequency:

    ```
    Router# show controllers cable slot/port downstream
    ```

  - Use the following command to verify the current value of an upstream port frequency:

    ```
    Router# show controllers cable slot/port upstream
    ```

  - Use the following command to check the value of the settings you entered:

    ```
    Router# show running-config
    ```

- To review changes you make to the configuration, use the EXEC **show startup-config** command to display the information stored in NVRAM.

## Viewing Sample Configuration Files

This section provides examples of Cisco uBR7200 series router configuration files. To view the current configuration of a Cisco uBR7200 series router, enter the **show running-config** command at the command-line interface (CLI) prompt in EXEC mode or privileged EXEC mode.

### Baseline Privacy Interface Configuration Files

The Cisco uBR7200 series CMTS supports 56-bit and 40-bit encryption and decryption; 56 bit is the default. After you choose a CMTS image that supports Baseline Privacy Interface (BPI), BPI is enabled by default for the Cisco uBR7200 series CMTS. Key commands that appear in the Cisco uBR7200 series router configuration file that denote that encryption and decryption are supported include:

- int cable 5/0
- cable privacy kek grace-time 800
- cable privacy kek life-time 750000
- cable privacy tek grace-time 800
- cable privacy tek life-time 56000
- cable privacy enable
- cable privacy mandatory

Note The cable interface must also support encryption and decryption.

When Baseline Privacy is enabled, the Cisco uBR7200 series router routes encrypted and decrypted packets from a host or peer to another host or peer. BPI is configured with key encryption keys (KEKs) and traffic encryption keys (TEKs). A KEK is assigned to a CM, based on the CM's service identifier (SID), and permits the CM to connect to the Cisco uBR7200 series router when Baseline Privacy is activated. The TEK is assigned to a CM when its KEK has been established. The TEK is used to encrypt data traffic between the CM and the Cisco uBR7200 series router.

KEKS and TEKs can be set for Baseline Privacy on the HFC network to expire based on a **grace-time** or a **life-time** value, defined in seconds. A **grace-time** value assigns a temporary key to a CM to access the network. A **life-time** value assigns a more permanent key to a CM. Each CM that has a **life-time** value assigned requests a new lifetime key from the Cisco uBR7200 series router before the current one expires.

To set the duration in *seconds* for KEK or TEK **grace-time** or **life-time**, use the following commands in global configuration mode. To restore the default values, use the **no** form of each command.

```
cable privacy kek {grace-time [seconds] | life-time [seconds]}
no cable privacy kek {grace-time | life-time}

cable privacy tek {grace-time [seconds] | life-time [seconds]}
no cable privacy tek {grace-time | life-time}
```

Syntax Description

| | |
|---|---|
| **grace-time** *seconds* | (Optional) Length of key encryption grace-time in seconds. Valid range is 300 to 1800 seconds. The default *grace-time* value is 600 seconds. |
| **life-time** *seconds* | (Optional) Length of the key encryption life-time in seconds.Valid range is 86,400 to 604,8000. The default *life-time* value is 604800 seconds. |

Tip Use the **show cable modem** command to identify a CM with encryption and decryption enabled. The *online(pk)* output of this command reveals a CM that is registered with BPI enabled and a KEK assigned. The *online(pt)* output reveals a CM that is registered with BPI enabled and a TEK assigned.

Should you want to change the Cisco uBR7200 series default of 56-bit encryption and decryption to 40-bit, use the "40 bit DES" option:

```
Router(config-if)# cable privacy ?
  40-bit-des           select 40 bit DES
  ^^^^^^^^^^
  authenticate-modem   turn on BPI modem authentication
  authorize-multicast  turn on BPI multicast authorization
  kek                  KEK Key Parms
  mandatory            force privacy be mandatory
  tek                  TEK Key Parms
```

Software then generates a 40-bit DES key, where the DES key that is generated and returned masks the first 16 bits of the 56-bit key to zero in software. To return to 56-bit encryption and decryption after changing to 40-bit, enter the **no** command in front of the "40 bit des" option.

# Configuring Cable Modem Interface Features

The cable interface in the Cisco uBR7200 series router supports downstream and upstream signals, and serves as the cable TV radio frequency (RF) interface. The downstream signal is output as an intermediate-frequency (IF) signal suitable for use with an external upconverter. Your cable plant, combined with your planned and installed subscriber base, service offering, and external network connections, determines the combination of cable interfaces, network uplink line cards, and other components that you should use.

The Cisco IOS software command-line interface (CLI) can be used to configure the Cisco cable interface line card for correct operation on the hybrid fiber-coaxial (HFC) cable network. This chapter describes the several required and optional tasks that configure the Cisco cable interface line card.

Note For additional information about CMs on the HFC network, refer to Chapter 5, "Managing Cable Modems on the Hybrid Fiber-Coaxial Network."

Perform the tasks in the following sections for required and optional cable interface configurations:

| Section | Description |
|---|---|
| "Configuring the Downstream Cable Modem Interface" section on page 3-2 | Provides instructions for performing required downstream configuration tasks. |
| "Configuring the Upstream Cable Modem Interface" section on page 3-11 | Provides instructions for performing required upstream configuration tasks. |
| "Configuring Optional Cable Modem Interface Features" section on page 3-28 | Provides instructions for performing several optional CM interface configurations. |

# Configuring the Downstream Cable Modem Interface

These configurations are required. The first step in configuring the Cisco CM interface is to configure the downstream cable interface. Configuring the downstream cable interface consists of the following procedures:

| Task | Description |
|---|---|
| "Activating Downstream Cable Address Resolution Protocol Requests" section on page 3-2 | Provides instructions to activate ARP requests on the cable interface so that the Cisco uBR7200 series CMTS can perform IP address resolution on the downstream path. |
| "Activating Downstream Ports" section on page 3-3 | Provides instructions to activate and verify a downstream port on a cable interface card for digital data transmissions over the HFC network. |
| "Assigning the Downstream Channel ID" section on page 3-5 | Provides instructions to assign and verify a numeric channel ID to the downstream port on the Cisco cable interface line card. |
| "Configuring Downstream Rate Limiting and Traffic Shaping" section on page 3-6 | Provides instructions for using the cable downstream rate-limit token-bucket command, which configures rate limiting and traffic shaping on the downstream channel. |
| "Setting the Downstream Helper Address" section on page 3-7 | Provides instructions to specify an IP address of a Dynamic Host Configuration Protocol (DHCP) server where User Datagram Protocol (UDP) broadcast packets will be sent. |
| "Setting the Downstream Interleave Depth" section on page 3-8 | Provides instructions to set the downstream interleave depth in milliseconds for the downstream port on the Cisco cable interface line card. |
| "Setting the Downstream Modulation" section on page 3-8 | Provides instructions to define the speed in symbols per second at which data travels downstream to the subscriber's CM. |
| "Setting the Downstream MPEG Framing Format" section on page 3-9 | Provides instructions to set and verify the downstream MPEG framing format, which must be compatible with DOCSIS specifications and your local cable plant operations. |
| "Setting Downstream Traffic Shaping" section on page 3-10 | Provides instructions to use the token bucket policing algorithm with traffic shaping options or the weighted discard algorithm to buffer, shape, or discard packets that exceed a set bandwidth. |

Note In most applications, default values for the commands used in these configuration steps are adequate to configure the Cisco uBR7200 series router. You do not need to specify individual parameters unless you want to deviate from system defaults.

For information on other configuration options, refer to the *Cisco Broadband Cable Command Reference Guide* on Cisco.com.

## Activating Downstream Cable Address Resolution Protocol Requests

This configuration is required. Address Resolution Protocol (ARP) is an Internet protocol used to map IP addresses to MAC addresses on computers and other equipment installed in a network. You must activate ARP requests on the cable interface so that the Cisco uBR7200 series CMTS can perform IP address resolution on the downstream path.

Note The default values for the commands used in this configuration step are adequate in most cases to configure the Cisco uBR7200 series CMTS.

To activate ARP requests, use the following command in cable interface configuration mode.

| Command | Purpose |
|---|---|
| `Router(config-if)# cable arp` | Enable ARP. This is the default. |

## Verifying ARP Requests

To verify that cable ARP is activated, enter the **more system:running-config** command and look for the cable interface configuration information. If ARP is activated, it does not appear in this output. If ARP is deactivated, it appears in the output as `no cable arp`.

```
Router# more system:running-config
Building configuration...

Current configuration:
!
interface cable5/0
ip address 1.1.1.1 255.255.255.0
 no keepalive
 no cable arp
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream symbol-rate 5056941
 cable upstream 0 frequency 15008000
 no cable upstream 0 shutdown
```

Tip If you are having difficulty with verification, verify that you entered the correct port and cable interface line card slot number when you activated ARP and when you entered the **show interface cable** command.

# Activating Downstream Ports

To activate a downstream port on a Cisco uBR7200 series cable interface card for digital data transmissions over the HFC network, complete the steps in the following table.

| | Command | Purpose |
|---|---|---|
| Step 1 | `Router> enable`<br>`Password: password`<br>`Router#` | Enters enable (privileged EXEC) mode.<br>Enter the password.<br>You have entered privileged EXEC mode when the prompt displays the pound symbol (`#`). |
| Step 2 | `Router# configure terminal`<br>`Enter configuration commands, one per line. End with CNTL/Z.`<br>`Router(config)#` | Enters global configuration mode. You have entered global configuration mode when the `(config)#` prompt appears.<br>This command can be abbreviated to **config t** or **conf t**. |

| | Command | Purpose |
|---|---|---|
| Step 3 | `Router(config)# interface cable5/0`<br>`Router(config-if)#` | Enters cable interface configuration mode.<br>In this example, the interface is downstream port 0 on the cable interface card installed in slot 1 of the Cisco uBR7200 series CMTS. |
| Step 4 | `Router(config-if)# cable downstream if-output` | Default. Activates downstream digital data from the Cisco uBR7200 series router. |
| | `Router(config-if)# no cable downstream if-output` | Deactivates downstream digital data. This command mutes the IF output of the cable interface card and shuts down the interfaces. |
| Step 5 | `Router(config-if)# no shutdown` | Places the downstream port in the "admin up" state. |
| Step 6 | `Router(config-if)# end`<br>`Router#` | Returns to privileged EXEC mode. |
| | `%SYS-5-CONFIG_I: Configured from console by console` | This message is normal and does not indicate an error. |

## Verifying the Downstream Ports

To determine if the downstream carrier is active (up), enter the **show controllers cable** command for the downstream port that you just configured. For National Television Standards Committee (NTSC) 6 MHz operations, see the following example:

```
Router# show controllers cable5/0 downstream
Cable5/0 Downstream is up
Frequency=96000000, Channel Width 6 MHz, 64-QAM, Symbol Rate 5.056941 Msps
 FEC ITU-T J.83 Annex B, R/S Interleave I=32, J=4
```

# Setting the Integrated Upconverter

The Cisco uBR7200 series router supports an integrated upconverter that outputs a DOCSIS RF signal on the DS0 RF downstream port. To enable the integrated upconverter, you must do the following:

- Set the downstream frequency—The integrated upconverter must be configured for the digital carrier frequency, which is the center frequency of the downstream RF carrier (the channel) for the downstream port. The **cable downstream frequency** command configures the downstream center frequency for the integrated upconverter.

Note The **cable downstream frequency** command has no effect on external upconverters. If you are using an external upconverter, this command is informational only and you must configure the external upconverter separately, using its own command procedures.

- Enable the integrated upconverter—The integrated upconverter is disabled by default and must be enabled with the **no cable downstream rf-shutdown** command.
- Enable the cable interface—The cable interface on the Cisco uBR7200 series router must be enabled before the integrated upconverter will output an RF signal.

To configure the integrated upconverter, use the following commands in cable interface configuration mode.

| Command | Purpose |
|---|---|
| `Router(config)# interface cable 1/0` | Enter interface configuration mode for the cable interface on the Cisco uBR7200 series router. |
| `Router(config-if)# cable downstream frequency down-freq-hz` | Enter the fixed center frequency for your downstream RF carrier in Hz. Allowable DOCSIS center frequencies are 91,000,000 to 857,000,000 Hz (the default is 500,000,000 Hz). |
| `Router(config-if)# no cable downstream rf-shutdown` | Enable the integrated upconverter. |
| `Router(config-if)# no shutdown` | Enable the cable interface. |

## Verifying the Integrated Upconverter Configuration

To verify the configuration for the integrated upconverter, enter the show controllers cable downstream command. The following is a typical display with a correctly configured center frequency:

```
Router# show controllers cable1/0 downstream
Cable1/0 Downstream is up
Frequency=525000000, Channel Width 6 MHz, 64-QAM, Symbol Rate 5.056941 Msps
FEC ITU-T J.83 Annex B, R/S Interleave I=32, J=4
Downstream channel ID: 0
```

Then enter the **show controllers cable** command, which also displays the center frequency, along with the power levels and whether the integrated upconverter is enabled. The following is a typical display when these values have been correctly configured:

```
Router# show controllers cable1/0
Interface Cable1/0
Hardware is IMC11
 BCM3210 revision=0x56B2
 Cable1/0 Upconverter is Enabled Output is Enabled
  Model: 74-2094-01 Serial Number: 0WAV04480010 CLEI Code:      CLEI#
  HW Rev:    PC2D0107 SW Rev: 007, NVRAM Rev: 006 ECI number 123456
  Downstream Frequency 525.0000 MHz
  IF Power 0.3 dBmv  RF Power 51.0 dBmv
...
```

If the center frequency has not been configured, the frequency is shown as “not set” as shown in the following example:

```
Router# show controllers cable1/0 downstream
Cable1/0 Downstream is up
Frequency is not set. Channel Width 6 MHz, 64-QAM, Symbol Rate 5.056941 Msps
FEC ITU-T J.83 Annex B, R/S Interleave I=32, J=4
Downstream channel ID: 0
```

If you are having trouble, make sure the cable connections are not loose or disconnected, and that you have calculated and entered the center frequency for your router accurately.

# Assigning the Downstream Channel ID

To assign a numeric channel ID to the downstream port on the Cisco cable interface line card, use the following command in cable interface configuration mode. The acceptable range is 0 to 255.

`Router(config-if)# cable downstream channel-id` *id*

Note The **cable downstream channel-id** command must be used with the following command:
`cable downstream frequency 54000000-1000000000 broadcast frequency - h`

These commands are used in instances where you want to send multiple downstream frequencies to a single region that contains CMs that can connect only to upstream ports on the same cable interface line card. You must configure unique channel IDs for each downstream that any CM is capable of receiving. The downstream frequency setting must match the setting on the upconverter.

Caution After defining unique downstream IDs, test the CMs for correct operation. Cisco recommends that when using this feature, you re-test each subsequent software release of CM code to verify correct operation and to ensure reasonable acquisition time for new installations. Failure to use these commands in conjunction or to test the involved CMs can result in customer service outages of indefinite duration.

### Verifying the Downstream Channel ID

To verify the downstream channel ID, enter the **show controllers cable** command for the downstream port you have just configured. See the following example:

```
Router# show controllers cable5/0 downstream
Cable5/0 Downstream is up
Frequency=96000000, Channel Width 6 MHz, 64-QAM, Symbol Rate 5.056941 Msps
FEC ITU-T J.83 Annex B, R/S Interleave I=32, J=4
Downstream channel ID: 1
```

## Configuring Downstream Rate Limiting and Traffic Shaping

To configure downstream traffic shaping, use the following command in cable interface configuration mode.

| Command | Purpose |
|---|---|
| `Router(config-if)#[no] cable downstream rate-limit token-bucket [shaping] weighted-discard [expwt <n>]` | Enables or disables rate limiting and traffic shaping on the downstream of a cable interface. |

Note Using Cisco IOS Release 12.0(5)T1 or higher, the software adds downstream calendar queuing routines and grant shaping application of the calendar queues.

Details for key command usage are provided below:

- To enable rate limiting on the given downstream port using the token bucket policing algorithm, issue the **cable downstream rate-limit token-bucket** command.
- To enable rate limiting on the given downstream port using the token bucket policing algorithm with traffic shaping, issue the **cable downstream rate-limit token-bucket shaping** command.
- To enable rate limiting on the given downstream port using the token bucket policing algorithm with a specific traffic shaping time granularity, issue the **cable downstream rate-limit token-bucket shaping granularity 8** command. Acceptable values are 1, 2, 4, 8, or 16 msecs.
- To enable rate limiting on the given downstream port using the token bucket policing algorithm with a specific maximum traffic shaping buffering delay, issue the **cable downstream rate-limit token-bucket shaping granularity 8** command. Acceptable values are 128, 256, 512, or 1028 msecs.

- To remove rate limiting on the given downstream port, issue the **cable downstream rate-limit token-bucket** command.
- To enable rate limiting on the given downstream port using a weighted packet discard policing algorithm and to assign a weight for the exponential moving average of loss rate value, issue the **cable downstream rate-limit weighted-discard 3** command. Acceptable values are 1 to 4.

# Setting the Downstream Helper Address

Specify an IP address of a Dynamic Host Configuration Protocol (DHCP) server where User Datagram Protocol (UDP) broadcast packets will be sent. You can specify a DHCP server for UDP broadcast packets from cable interfaces, and a DHCP server for UDP broadcast packets from hosts. To set a downstream helper address, use the following commands in cable interface configuration mode.

| | Command | Purpose |
|---|---|---|
| Step 1 | `Router(config-if)# cable helper-address 10.x.x.x cable-modem` | Set the downstream helper address to the DHCP server at IP address 10.*x.x.x* for UDP broadcast packets from cable modems.<br>Note Use the IP address of the DHCP server. Both 10.*x.x.x* and 172.56.*x.x* are private ranges. |
| Step 2 | `Router(config-if)# cable helper-address 172.56.x.x host` | Set the downstream helper address to the DHCP server at IP address 172.56.*x.x* for UDP broadcast packets from hosts. |

## Verifying the Downstream Helper Address

To verify the downstream helper address setting, enter the **show running-config** command and look for `cable helper-address` in the cable interface configuration information:

```
Router# show running-config
Building configuration...

Current configuration:
!
interface cable5/0
ip address 10.254.254.254 255.0.0.0
 no ip directed-broadcast
 cable helper-address 192.168.1.1
 no keepalive
```

Perform these steps if you are having difficulty with verification:

Step 1 Check the cables, upconverters, RF levels, and frequencies if the cable interfaces do not find a downstream signal.

Step 2 Check the cables, RF levels, and upstream frequencies, and enter a **no shut** command if the cable interfaces find a downstream signal, but not an upstream signal.

Step 3 Check the provisioning servers.

- Ping the DHCP server using the source IP address option—the primary IP address of a cable interface.
- Check IP routing if the cable interfaces acquire an RF upstream and downstream lock, but do not stay up.

Step 4 Check DHCP options and the IP address of the Time-of-Day (ToD) server:

- Ping the ToD server using the source IP address option.
- Check IP routing.

- Verify that the TFTP filename is correct.
- Verify that the TFTP file is in the correct directory on the TFTP server.
- Ensure that the TFTP file has read privileges.
- Ping the TFTP server using the source IP address option, and check IP routing if the cable interfaces acquire an RF and a DHCP, but fail on ToD or TFTP.

# Setting the Downstream Interleave Depth

Set the interleave depth for the downstream port on the Cisco cable interface line card. A higher interleave depth provides more protection from bursts of noise on the HFC network; however, it increases downstream latency.

Note The valid values are 8, 16, 32 (default), 64, and 128.

To set the downstream interleave depth in milliseconds, use the following command in cable interface configuration mode:

```
Router(config-if)# cable downstream interleave-depth {8|16|32|64|128}
```

## Verifying the Downstream Interleave Depth

To verify the downstream interleave depth setting, enter the **show controllers cable** command for the downstream port you have just configured:

```
Router# show controllers cable5/0 downstream
Cable5/0 Downstream is up
 Frequency=96000000, Channel Width 6 MHz, 64-QAM, Symbol Rate 5.056941 Msps
 FEC ITU-T J.83 Annex B, R/S Interleave I=32, J=
```

Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected.

Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.

Step 3 Ensure that the captive installation screws are tight.

Step 4 Verify that you have entered the correct slot and port numbers.

Step 5 Verify that the downstream carrier is active, using the **cable downstream if-output** command.

# Setting the Downstream Modulation

To set the downstream modulation, define the speed in symbols per second at which data travels downstream to the subscriber's CM. A symbol is the basic unit of modulation. Quadrature Phase Shift Key (QPSK) encodes 2 bits per symbol, Quadrature Amplitude Modulation (QAM) -16 encodes 4 bits per symbol, QAM-64 encodes 6 bits per symbol, and QAM-256 encodes 8 bits per symbol.

Note Setting a downstream modulation rate of QAM-256 requires approximately a 6 dB higher signal-to-noise ratio (SNR) than QAM-64 at the subscriber's cable interface. If your network is marginal or unreliable at QAM-256, use the QAM-64 format instead. Also, consider the significance of your data.

To set the downstream modulation, use the following command in cable interface configuration mode. The standard DOCSIS modulation rate (and the Cisco default) is QAM-64.

```
Router(config-if)# cable downstream modulation 64qam
```

## Verifying the Downstream Modulation

To verify the downstream modulation setting, enter the **show controllers cable** command for the downstream port you have just configured. See the following example:

```
Router# show controllers cable5/0 downstream
Cable5/0 Downstream is up
 Frequency=96000000, Channel Width 6 MHz, 64-QAM, Symbol Rate 5.056941 Msps
 FEC ITU-T J.83 Annex B, R/S Interleave I=32, J=4
```

Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected.

Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.

Step 3 Ensure that the captive installation screws are tight.

Step 4 Verify that you have entered the correct slot and port numbers

Step 5 Verify that the downstream carrier is active, using the **cable downstream if-output** command

Step 6 Verify that you have selected the default if you are not certain about the modulation rate needed.

# Setting the Downstream MPEG Framing Format

The MPEG framing format must be compatible with DOCSIS specifications at http://www.cablemodem.com/specifications.html and your local cable plant operations.

Tip Annex B is the DOCSIS MPEG framing format standard for North America.

Note Annex B framing format is automatically set when configuring Cisco cable interface line cards. The cable interface line card's downstream ports and the connected CMs on the network must be set to the same MPEG framing format and must support DOCSIS operations as appropriate.

The following command appears in the Cisco uBR7200 series router configuration file to designate Annex B operation. This command sets the downstream MPEG framing format.

```
Router(config-if)# cable downstream annex {B}
```

## Verifying the Downstream MPEG Framing Format

To verify the downstream MPEG framing format setting, enter the **show controllers cable** command for the downstream port you have just configured. See the following example:

```
Router# show controllers cable5/0 downstream
Cable5/0 Downstream is up
Frequency=96000000, Channel Width 6 MHz, 64-QAM, Symbol Rate 5.056941 Msps
FEC ITU-T J.83 Annex B, R/S Interleave I=32, J=4
Downstream channel ID: 0
```

# Setting Downstream Traffic Shaping

Downstream traffic shaping enables you to use the token bucket policing algorithm with traffic shaping options or the weighted discard algorithm to buffer, shape, or discard packets that exceed a set bandwidth. Downstream traffic shaping is disabled by default.

To enable downstream traffic shaping for a downstream port on a Cisco cable interface line card, use one of the following commands in cable interface configuration mode.

## Verifying Downstream Traffic shaping

| | Command | Purpose |
|---|---|---|
| Step 1 | `Router(config-if)# cable downstream rate-limit token-bucket` | Enables traffic shaping on the downstream port using the token bucket policing algorithm. With this command, the Cisco uBR7200 series router automatically drops packets that are in violation of the allowable bandwidth. |
| | `Router(config-if)# cable downstream rate-limit token-bucket shaping` | Enables traffic shaping on the downstream port using the token bucket policing algorithm with traffic shaping. |
| | `Router(config-if)# cable downstream rate-limit token-bucket shaping granularity 8` | Enables traffic shaping on the downstream port using the token bucket policing algorithm with specific traffic shaping time granularity. Acceptable values are 1, 2, 4, 8, or 16 milliseconds. |
| | `Router(config-if)# cable downstream rate-limit token-bucket shaping max-delay 256` | Enables traffic shaping on the downstream port using the token bucket policing algorithm with specific maximum traffic shaping buffering delay. Acceptable values are 128, 256, 512, or 1028 milliseconds. |
| Step 2 | `Router(config-if)# cable downstream rate-limit weighted-discard 3` | Enables traffic shaping on the downstream port using the weighted discard algorithm and assigns a weight for the exponential moving average of the loss rate. Acceptable values are 1 to 4. |
| Step 3 | `Router(config-if)# ^Z`<br>`Router#` | Exits back to EXEC mode so that you can verify the steps. |

To determine if downstream traffic shaping is configured and activated, enter the **show running-config** command and look for the cable interface configuration information. If downstream traffic shaping is configured and enabled, a traffic shaping entry appears in the output. If downstream traffic shaping is disabled, no traffic shaping entry appears.

```
Router# show running-config
```

```
Building configuration...
Current configuration:
!
interface cable5/0
ip address 10.254.254.254 255.0.0.0
no ip directed-broadcast
cable helper-address 192.168.1.1
no keepalive
cable downstream annex B
cable downstream modulation 64qam
```

Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected.

Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.

Step 3 Ensure that the captive installation screws are tight.

Step 4 Verify that you have entered the correct slot and port numbers.

Step 5 Verify that you selected the default if you are not certain about the modulation rate needed.

Step 6 Verify that the downstream carrier is active using the **cable downstream if-output** command.

# Configuring the Upstream Cable Modem Interface

These configurations are required. Upstream cable interface commands configure the frequency and input power level of the upstream signal, in addition to error detection and correction of the upstream signal. The configuration of the upstream cable interface depends on the characteristics of your cable plant.

Perform the following tasks in this section to configure the upstream cable interface.

Note For some of these tasks, default values are adequate to configure the device.

| Task | Description |
|---|---|
| "Activating Upstream Admission Control" section on page 3-12 | Provides information about the upstream admission control feature, and provides instructions to set the upstream admission control as a percentage of the upstream channel capacity. |
| "Activating Upstream Differential Encoding" section on page 3-13 | Provides brief explanation and instructions to activate differential encoding on the upstream, which is a digital encoding technique whereby a binary value is denoted by a signal change rather than a particular signal level. |
| "Activating Upstream Forward Error Correction" section on page 3-14 | Provides instructions to activate forward error correction (FEC). The Cisco uBR7200 series CMTS uses FEC to attempt to correct any upstream data that might have been corrupted. |
| "Activating the Upstream Ports" section on page 3-15 | Provides instructions to activate upstream ports. Each upstream port must be activated to enable upstream data transmission from the CMs on the HFC network to the Cisco uBR7200 series CMTS. |

| Task | Description |
|---|---|
| "Activating Upstream Power Adjustment" section on page 3-16 | Provides instructions to enable upstream power adjustment. This feature sets the minimum power adjustment in dB that will allow continued ranging status. |
| "Activating the Upstream Scrambler" section on page 3-17 | Provides instructions to activate the upstream scrambler on the upstream RF carrier, which enables CMs on the HFC network to use built-in scrambler circuitry for upstream data transmissions. |
| "Activating Upstream Timing Adjustment" section on page 3-17 | Provides instructions to activate upstream timing adjustment on the specified interface. This feature sets the minimum timing adjustment that allows continued ranging status. |
| "Configuring Upstream Rate Limiting and Traffic Shaping" section on page 3-18 | Provides instructions to configure upstream rate limiting and traffic shaping, which delays the scheduling of the upstream packet. In turn, this causes the packet to be buffered on the cable CPE device, instead of being dropped. |
| "Setting Upstream Backoff Values" section on page 3-19 | Provides DOCSIS-compliant instructions that define contention resolution for CMs wanting to transmit data or requests on the upstream channel. Contention resolution is achieved with a truncated binary exponential backoff value. |
| "Setting the Upstream Channel Width" section on page 3-21 | Provides instructions to enter the upstream channel width in hertz (Hz). Also describes NTSC spectrum parameters and spectrum management processes. |
| "Setting the Upstream Frequency" section on page 3-22 | Provides instructions to set upstream channel frequency for the RF output that complies with the expected input frequency of the Cisco cable interface line card. |
| "Setting the Upstream Input Power Level" section on page 3-24 | Provides instructions to set the upstream input power level in decibels per millivolt (dBmV), and provides additional information about the Cisco uBR7200 series controls the output power levels of CMs |
| "Setting Upstream Traffic Shaping" section on page 3-26 | Provides instructions to activate traffic shaping on the upstream. Upstream traffic shaping, available on the DOCSIS upstream channel, delays the scheduling of the upstream packet, which in turn causes the packet to be buffered on the cable customer premises equipment (CPE) device, instead of being dropped. |
| "Specifying Upstream Minislot Size" section on page 3-25 | Provides instructions to specify the minislot size (in ticks) for specific upstream cable interfaces. The minislot size and the channel width are related to certain degree but not tightly coupled. |

# Activating Upstream Admission Control

Upstream admission control tallies up the total amount of guaranteed minimum upstream throughput reserved by CMs on an upstream interface. Once the total exceeds an allowable level, no more CMs requiring a guaranteed minimum upstream rate are allowed online on that upstream port.

Cisco CMTS upstream admission control is turned off by default and must be activated. To set the upstream admission control as a percentage of the upstream channel capacity, use the following command in cable interface configuration mode. The admission control is set as a percentage of the specified upstream channel capacity. The acceptable range is from 10 to 1000 percent.

```
Router(config-if)# cable upstream usport admission-control percentage
```

For example:

```
7246VXR(config-if)#cable upstream 0 admission-control ?
    Max Reservation Limit As Percentage of Raw Channel Capacity
```

Syntax Description

| | |
|---|---|
| usport | The upstream port that has admission control enabled. |
| percentage | The optional *percentage* parameter specifies the overbooking rate that will be used when deciding the amount of bandwidth that is available to be guaranteed. |

Note If *percentage* is left blank or set to 100%, the CMTS will only allow a total up to the real available upstream bandwidth to be guaranteed. If percentage is set to its maximum of 1000, then up to 10 times the real interface bandwidth may be "guaranteed".

## Verifying Upstream Admission Control

To determine if upstream admission control is configured and activated, enter the **show running-config** command in privileged EXEC mode and look for the cable interface configuration information. If upstream admission control is configured and enabled, an admission control entry appears in the **show running-config** command output, indicating the user-defined percentage of upstream channel capacity allowable. If upstream admission control is disabled, no admission control entry appears in the output.

Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected.

Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.

Step 3 Ensure that the captive installation screws are tight.

Step 4 Verify that you have entered the correct slot and port numbers.

Step 5 Verify that you selected a valid frequency for your router.

# Activating Upstream Differential Encoding

Differential encoding on the upstream is a digital encoding technique whereby a binary value is denoted by a signal change rather than a particular signal level. To enable differential encoding on upstream traffic to a specified cable interface, use the following command in cable interface configuration mode. Upstream differential encoding is enabled by default.

```
Router(config-if)# cable upstream usport differential-encoding
```

## Verifying Upstream Differential Encoding

To determine if upstream differential encoding is activated, enter the **show running-config** command and look for the cable interface configuration information. If upstream differential encoding is enabled, a differential encoding entry appears in the **show running-config** output. If upstream differential encoding is disabled, no differential encoding entry appears in the output.

Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected.

Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.

Step 3 Ensure that the captive installation screws are tight.

Step 4 Verify that you have entered the correct slot and port numbers.

Step 5 Verify that you selected a valid frequency for your router.

# Activating Upstream Forward Error Correction

The Cisco uBR7200 series CMTS uses forward error correction (FEC) to attempt to correct any upstream data that might have been corrupted. When FEC is activated, all CMs on the network also activate FEC.

Note Although upstream FEC is an option, Cisco recommends that you use upstream FEC. FEC is activated by default and should not be disabled.

To activate the upstream forward error correction and to enable FEC, use the following command in cable interface configuration mode.

```
Router(config-if)# cable upstream usport fec
```

## Verifying Upstream FEC

To verify whether FEC is activated or deactivated, enter the **more system:running-config** command and look for the cable interface configuration information. If FEC is enabled, an FEC entry appears in the **show running-config command** output. If FEC is disabled, no FEC entry appears in the output.

Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected.

Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.

Step 3 Ensure that the captive installation screws are tight.

Step 4 Verify that you have entered the correct slot and port numbers.

Step 5 Verify that you selected a valid frequency for your router.

# Activating the Upstream Ports

Each upstream port must be activated to enable upstream data transmission from the CMs on the HFC network to the Cisco uBR7200 series CMTS.

Note The upstream cable interface does not operate until you either set a fixed upstream frequency or create and configure a spectrum group. Refer to the "Setting the Upstream Frequency" section on page 3-22 for details.

To activate the upstream ports, use the following commands in global configuration mode.

| | Command | Purpose |
|---|---|---|
| Step 1 | `Router(config)# interface cable slot/port` | Specifies a cable interface and enters cable interface configuration mode. |
| Step 2 | `Router(config-if)# no cable upstream usport shutdown` | Enables upstream data traffic. |

## Verifying the Upstream Ports

To determine if the upstream ports are activated or deactivated, enter the **show interface cable** command for the upstream port just configured:

```
Router# show interface cable5/0
Cable5/0 is up, line protocol is up
 Hardware is BCM3210 FPGA, address is 00e0.1e5f.7a60 (bia 00e0.1e5f.7a60)
 Internet address is 1.1.1.3/24
 MTU 1500 bytes, BW 27000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
 Encapsulation, loopback not set, keepalive not set
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input 00:00:25, output 00:00:00, output hang never
 Last clearing of "show interface" counters never
 Queuing strategy: fifo
 Output queue 0/40, 0 drops; input queue 0/75, 0 drops
 5 minute input rate 0 bits/sea, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
     10878 packets input, 853740 bytes, 0 no buffer
     Received 3679 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     5401 packets output, 645885 bytes, 0 underruns
     0 output errors, 0 collisions, 9 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

# Activating Upstream Frequency Adjustment

To enable automatic upstream frequency adjustment for a specified cable interface, use the following commands in cable interface configuration mode.

| | Command | Purpose |
|---|---|---|
| Step 1 | `Router(config-if)# cable upstream` *usport* `frequency-adjust averaging` *percentage* | Set the minimum number of frequency adjustment packets required to justify changing the upstream frequency adjustment method as a percentage. Acceptable range is 10 to 100 percent. Default = 30 percent. |
| Step 2 | `Router(config-if)# end` `Router#` | Return to enable (privileged EXEC) mode. |

To return the automatic upstream frequency adjustment percentage to the default value of 30 percent, enter the following command in cable interface configuration mode:

```
Router(config-if)# no cable upstream usport frequency-adjust averaging
```

## Verifying Upstream Frequency Adjustment

To determine if upstream frequency adjustment is configured and activated, enter the **show running-config** command and look for the cable interface configuration information. If upstream frequency adjustment is enabled, frequency adjustment entries are displayed in the **show running-config** output. If frequency adjustments are disabled, no frequency adjustment entry displays in the output.

Perform these steps if you are having difficulty with verification:

1. Ensure the cable connections are not loose or disconnected
2. Ensure the cable interface line card is firmly seated in its chassis slot.
3. Ensure the captive installation screws are tight.
4. Verify that you have entered the correct slot and port numbers; you selected a valid frequency for your router.

# Activating Upstream Power Adjustment

To enable upstream power adjustment for a specified cable interface, use one of the following commands in cable interface configuration mode.

| Command | Purpose |
|---|---|
| `Router(config-if)# cable upstream` ***usport*** `power-adjust continue` *db* | Sets the minimum power adjustment in dB that allows continued ranging status. Valid values are 2 to 15 dB. Default = 2 dB. |
| `Router(config-if)# cable upstream` ***usport*** `power-adjust noise` *percentage* | Sets the minimum number (percentage) of power-adjustment packets required to justify changing the upstream power rating. Valid values are 10 to 100 percent. Default = 30 percent. |
| `Router(config-if)# cable upstream 0 power-adjust threshold` *db* | Sets the power-adjustment threshold in dB. Valid values are 0 to 2 dB. Default = 1 dB. |
| `Router(config-if)# end` `Router#` | Returns to enable (privileged EXEC) mode. |

To return the automatic upstream power-adjustment ranging value to the default of 2 dB, enter the following command in cable interface configuration mode:

```
Router(config-if)# no cable upstream usport power-adjust continue
```

To return the automatic upstream power-adjustment noise value to the default of 30 percent, enter the following command in cable interface configuration mode:

```
Router(config-if)# no cable upstream usport power-adjust noise
```

To return the upstream power-adjustment threshold value to the default of 1 dB, enter the following command in cable interface configuration mode:

```
Router(config-if)# no cable upstream usport power-adjust threshold
```

### Verifying Upstream Power Adjustment

To determine if upstream power adjustment is configured and activated, enter the **show running-config** command and look for the cable interface configuration information. If upstream power adjustment is enabled, any or all three of the **continue**, **noise**, and **threshold** power-adjustment entries appear in the **show running-config** command output. If all three upstream power adjustments are disabled, no power-adjustment entry appears in the **show running-config** command output.

## Activating the Upstream Scrambler

The scrambler on the upstream RF carrier enables CMs on the HFC network to use built-in scrambler circuitry for upstream data transmissions. The scrambler circuitry improves reliability of the upstream receiver on the cable interface line card.

Caution The upstream scrambler is activated by default and should not be disabled under normal circumstances. Disabling it can result in corrupted packets. Disable it only for prototype modems that do not support the upstream scrambler.

To activate the upstream scrambler, use the following command in cable interface configuration mode. The upstream scrambler is enabled by default.

```
Router(config-if)# cable upstream usport scrambler
```

### Verifying the Upstream Scrambler

To determine if the upstream scrambler is activated, enter the **more system:running-config** command and look for the cable interface configuration information. Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected.
Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.
Step 3 Ensure that the captive installation screws are tight.
Step 4 Verify that you have entered the correct slot and port numbers.
Step 5 Verify that you selected a valid frequency for your router.

## Activating Upstream Timing Adjustment

To enable upstream timing adjustment for a specified cable interface, use one of the following commands in cable interface configuration mode.

| Command | Purpose |
|---|---|
| `Router(config-if)# cable upstream` ***usport*** `time-adjust continue` *seconds* | Sets the minimum timing adjustment that allows continued ranging status. Valid *second* values are 2 to 64 seconds. Default = 2 seconds. |
| `Router(config-if)# cable upstream` ***usport*** `time-adjust threshold` *seconds* | Sets the timing adjustment threshold value in seconds. Valid *second* values are 1to 32 seconds. Default = 1 second. |
| `Router(config-if)# end`<br>`Router#` | Returns to enable (privileged EXEC) mode. |

To return the upstream time-adjustment ranging value to the default of 2 seconds, enter the following command in cable interface configuration mode:

```
Router(config-if)# no cable upstream usport time-adjust continue
```

To return the upstream time adjustment threshold value to the default of 1 second, enter the following command in cable interface configuration mode:

```
Router(config-if)# no cable upstream usport time-adjust threshold
```

## Verifying Upstream Timing Adjustment

To determine if upstream timing adjustment is configured and activated, enter the **show running-config** command and look for the cable interface configuration information. If upstream timing adjustment is enabled, either or both of the **continue** and **threshold** timing-adjustment entries appear in the **show running-config** command output. If both the **continue** and **threshold** upstream timing adjustments are disabled, no timing adjustment entry appears in the **show running-config** command output.

Tip Perform the following steps if you are having difficulty with verification:

Step 1 Verify that the cable connections are not loose or disconnected.

Step 2 Verify that the cable interface line card is firmly seated in its chassis slot

Step 3 Verify that the captive installation screws are tight.

Step 4 Confirm that you have entered the correct slot and port numbers.

# Configuring Upstream Rate Limiting and Traffic Shaping

You can configure rate limiting and traffic shaping on a DOCSIS upstream channel. This delays the scheduling of the upstream packet, which in turn causes the packet to be buffered on the cable CPE device, instead of being dropped. This allows the user's TCP/IP stack to pace the application traffic appropriately and approach throughput commensurate with the subscriber's defined QoS levels.

To configure this, use the following command in cable interface configuration mode.

| Command | Purpose |
|---|---|
| `Router(config-if)#`*`[no]`* `cable upstream` <*n1*> `rate-limit [token-bucket]` | Enables or disables DOCSIS rate limiting or shaping on an upstream channel. <n1> depends on the number of upstream channels on the specific cable interface line card. |

Using Cisco IOS Release 12.0(5)T1 or higher, the software supports:

- Generic calendar queuing routines
- New token bucket policing function
- Grant shaping application of the calendar queues
- Upstream rate shaping option to the token-bucket keyword
- A default state change from 1 second burst policing to token-bucket with shaping

Tip Upstream grant shaping is per CM (SID). Shaping can be enabled or disabled for the token-bucket algorithm.

Note Before the introduction of this feature, the CMTS would drop bandwidth requests from a CM it detected as exceeding its configured peak upstream rate. Such request dropping affects the throughput performance of IP-based protocols such as FTP, TCP, and SMTP. With this feature, the CMTS can shape (buffer) the grants for a CM that is exceeding its upstream rate, rather than dropping the bandwidth requests.

```
Router# show interface c3/0 sid 1 counters
Sid   Inpackets  Inoctets   Outpackets Outoctets  Ratelimit  Ratelimit
                                                  BWReqDrop  DSPktDrop
1     67859      99158800   67570      98734862   2579       0
```

# Setting Upstream Backoff Values

The DOCSIS-specified method of contention resolution for CMs wanting to transmit data or requests on the upstream channel is a truncated binary exponential backoff value, with the initial backoff window and the maximum backoff window controlled by the CMTS. The Cisco uBR7200 series CMTS specifies backoff window values for both data and initial ranging, and sends these values downstream as part of the Bandwidth Allocation Map (MAP) MAC message.

The values are configurable on the Cisco uBR7200 series software and are power-of-two values. For example, a value of 4 indicates a window between 0 and 15; a value of 10 indicates a window between 0 and 1023. You can set fixed start and end values for data backoff on the upstream ports, or you can set the upstream ports for automatic data backoff. You have the same options for ranging backoff. For both backoff windows, the default start value is 0; the default end value is 4. Valid values are from 0 to 15.

Note Cisco does not recommend that you adjust default values, but that you enable the automatic dynamic backoff algorithm. Refer to the "Configuring Dynamic Contention Algorithms (Cable Insertion Interval, Range, and Data Backoff)" section on page 5-6.

To set data or ranging backoff values for an upstream port, use one or more of the following commands in cable interface configuration mode.

| | Command | Purpose |
|---|---|---|
| Step 1 | `Router(config-if)# cable upstream` *usport* `data-backoff` *start end*<br><br>or<br><br>`Router(config-if)# cable upstream` *usport* `data-backoff automatic` | Optimizes the **automatic** setting for as many as 250 cable interfaces per upstream port. Sets manual values for data backoff windows only when operating with more than 250 cable interfaces per upstream port.<br><br>Configures the default backoff window values of 0 and 4. |
| Step 2 | `Router(config-if)# cable upstream` *usport* `range` *start end*<br><br>or<br><br>`Router(config-if)# cable upstream` *usport* `range automatic` | Optimizes the **automatic** setting for as many as 250 cable interfaces per upstream port. Sets manual values for data backoff windows only when operating with more than 250 cable interfaces per upstream port.<br><br>Configures the default backoff window values of 0 and 4. |

When considering whether to adjust backoff values, keep the following considerations in mind:

- The cable interface reconnection time after a power outage is related to the following factors:
  - DHCP, ToD, and TFTP servers often operate well below 1 percent load under normal situations, but can jump to over 100 percent after an outage.
  - Adjusting the backoffs to larger numbers slows cable interface reconnection and reduces server load.
  - Backoffs that are too small result in cable interfaces failing to range the upstream RF levels correctly and cycling to maximum power, thus increasing connection time and reducing network performance.
  - Backoffs that are too large result in increased recovery time after a large service outage.
  - There is significant variation in cable interface performance (brand to brand) in cable interface restart time.
- All cable interfaces should recover in 0 to 10 minutes after all services are restored (Cisco uBR7200 series, RF transport, DHCP, TFTP, and ToD servers). A CM that takes longer than 10 minutes could be experiencing a problem with the modem itself, a problem with CMTS settings, or a problem in the DOCSIS provisioning servers.

Note Upstream segments serving a relatively large number of cable interfaces (for example, more than 1600) might suffer recovery times greater than 10 minutes.

## Verifying Upstream Data Backoff

To verify backoff window settings, enter the **show controllers cable** command for the upstream port you have just configured:

```
Router# show controllers cable5/0 u0
Cable5/0 Upstream 0 is up
Frequency 24.016 MHz, Channel Width 1.600 MHz, QPSK Symbol Rate 1.280 Msps
  Spectrum Group is overridden
  SNR 33.2560 dB
  Nominal Input Power Level 0 dBmV, Tx Timing Offset 2288
  Ranging Backoff automatic (Start 0, End 3)
  Ranging Insertion Interval automatic (60 ms)
  Tx Backoff Start 0, Tx Backoff End 4
  Modulation Profile Group 1
  part_id=0x3137, rev_id=0x03, rev2_id=0xFF
  nb_agc_thr=0x0000, nb_agc_nom=0x0000
  Range Load Reg Size=0x58
  Request Load Reg Size=0x0E
```

```
Minislot Size in number of Timebase Ticks is = 8
Minislot Size in Symbols = 64
Bandwidth Requests = 0xFE
Piggyback Requests = 0xD
Invalid BW Requests= 0x2
Minislots Requested= 0x2963
Minislots Granted  = 0x2963
Minislot Size in Bytes = 16
Map Advance = 4000 usecs
UCD Count = 32964
DES Ctrl Reg#0 = C000C043, Reg#1 = 0
```

## Setting the Upstream Channel Width

Use the commands below to enter the upstream channel width in hertz (Hz). For NTSC operations, valid values are 200000 Hz (160 kilo symbols per second [ksps]), 400,000 Hz (320 ksps), 800,000 Hz (640 ksps), 1,600,000 Hz (1280 ksps), and 3,200,000 Hz (2560 ksps). The default is 1,600,000 Hz.

If no acceptable channels of the specified width are found, the spectrum management card automatically begins to scan the upstream spectrum for the next largest available channel width; for example, if the spectrum management card is unable to find a usable 1.6 MHz upstream channel, it automatically begins searching for usable 800 kHz channels.

Caution Higher symbol rates are more susceptible to RF noise and interference. If you use a symbol rate or modulation format beyond the capabilities of your HFC network, you might experience packet loss or loss of cable interface connectivity.

Note For QAM-16 channel widths of 400 kHz (320 ksps) or greater, Cisco recommends that you use QAM-16 modulation for long and short data, and that you use QPSK for request, initial, and station communications. For QAM-16 channel widths of 200 kHz (160 ksps), all communication must be able to use QAM-16. That is, 160 ksps with QAM-16 requires an exceptional signal-to-noise ratio (SNR) in your upstream channels. When you use QAM-16 for request, initial, and station maintenance messages with channel widths greater than 400 kHz, the QAM-16 preamble and message data take longer to transmit than the QPSK format.

Note To set the upstream channel width, use the following commands in cable interface configuration mode.

| | Command | Purpose |
|---|---|---|
| Step 1 | `Router(config-if)# cable upstream` *usport* `channel-width` *width* | Enters the channel width for your upstream RF carrier in Hz. |
| Step 2 | `Router(config-if)# no cable upstream` *usport* `channel-width` | Returns the channel width to its default setting of 1,600,000 Hz. |

For additional information about channel width and minislot size, refer to the *Cable Radio Frequency (RF) FAQs* on Cisco.com.

## Verifying Upstream Channel Width

To verify the current value of the upstream channel width, enter the **show controllers cable** command for the upstream port you just configured. A sample follows below:

```
Router# show controllers cable5/0 u0
Cable5/0 Upstream 0 is up
  Frequency 24.016 MHz, Channel Width 0.800 MHz, QPSK Symbol Rate 0.640 Msps
```

```
Spectrum Group is overridden
SNR 33.2560 dB
Nominal Input Power Level 0 dBmV, Tx Timing Offset 2288
Ranging Backoff automatic (Start 0, End 3)
Ranging Insertion Interval automatic (60 ms)
Tx Backoff Start 0, Tx Backoff End 4
Modulation Profile Group 1
```

Perform these steps if you are having difficulty with verification:

Step 1 Use a valid combination of modulation format (QPSK and QAM-16), minislot size, frequency, and the **no shutdown** command.

Step 2 Use a recommended or previously tested modulation profile. It is not uncommon to create a modulation profile that does not allow cable interface-to-headend communication. Because each message type is individually specified, some messages might not work.

Step 3 Verify using IP ping packets of varying lengths (64 to 1500 bytes). Ping from the headend to the cable interface.

Step 4 Verify with your cable interface vendor that your CM software is fully certified or compatible with DOCSIS 1.0 and extensions, as appropriate.

# Setting the Upstream Frequency

The upstream channel frequency of your RF output must be set to comply with the expected input frequency of your Cisco cable interface line card. To configure upstream channel frequencies, perform one of the following tasks:

- Configure a fixed frequency from 5 to 42 MHz for NTSC operations, then enable the upstream port.
- Create a global spectrum group, assign the interface to it, and enable the upstream port.

Note You can also select a default that does not set a specific fixed value.

Note The upstream port is frequency agile. If you define spectrum groups, the frequency can change while the interface is up and carrying traffic.

A modulation profile consists of a table of physical layer characteristics for the different types of upstream bursts; for example, initial maintenance, long grant, request/data, request, short grant, and station maintenance.

Note The upstream cable interface does not operate until you either set a fixed upstream frequency or create and configure a spectrum group.

If you are setting a fixed upstream frequency, make sure that the frequency selected does not interfere with the frequencies used for any other upstream applications running on the cable plant.

To set a fixed upstream frequency, use the following commands in cable interface configuration mode.

| | Command | Purpose |
|---|---|---|
| Step 1 | `Router(config-if)# cable upstream usport frequency up-freq-hz` | Enters the fixed center frequency for your upstream RF carrier in Hz. |
| Step 2 | `Router(config-if)# no cable upstream usport shutdown` | Places the upstream port in the "admin up" state. |

Tip For National Television Standards Committee (NTSC) operations, valid ranges are 5000000 to 42000000 Hz.

Caution Some cable systems cannot reliably transport frequencies near these band edges. The wider the upstream channel (in MHz), the more difficulty you might have. Enter a center frequency between 20 and 38 MHz if you have difficulty.

Note You can also select a default that does not set a specific fixed value. The Cisco uBR7200 series software instructs the cable interfaces to use this frequency as the center frequency.

## Verifying the Upstream Frequency

To verify the current value of the upstream frequency, enter the **show controllers cable** command for the upstream port you have just configured:

```
Router# show controllers cable5/0 u0
Cable5/0 Upstream 0 is up
Frequency 24.016 MHz, Channel Width 1.600 MHz, QPSK Symbol Rate 1.280 Msps
  Spectrum Group is overridden
  SNR 33.2560 dB
  Nominal Input Power Level 0 dBmV, Tx Timing Offset 2288
  Ranging Backoff automatic (Start 0, End 3)
  Ranging Insertion Interval automatic (60 ms)
  Tx Backoff Start 0, Tx Backoff End 4
  Modulation Profile Group 1
```

Note The upstream frequency displayed in the **show controllers cable** command output might not match the frequency that you entered when you set the upstream frequency. The Cisco uBR7200 series CMTS might select an upstream frequency close to the frequency you entered that offers better performance. The Cisco uBR7200 series CMTS selects the closest frequency available.

Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected

Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.

Step 3 Ensure that the captive installation screws are tight.

Step 4 Verify that you have entered the correct slot and port numbers.

Step 5 Verify that you have selected a valid frequency for your router.

# Setting the Upstream Input Power Level

The Cisco uBR7200 series CMTS controls the output power levels of CMs to meet the desired upstream input power level. The nominal input power level for the upstream RF carrier is specified in decibels per millivolt (dBmV). The default setting of 0 dBmV is the optimal setting for the upstream power level.

The valid range for the input power level depends on the data rate. At 1.6 MHz, the valid range is –10 to 25 dBmV. If your power levels operate at greater than the maximum valid level, use an inline attenuator to bring the power level to within the valid range.

Caution If you increase the input power level, CMs on your HFC network increase their transmit power level. This increases the carrier-to-noise ratio (C/N) on the network, but also increases distortion products. Composite Second Order Beat (CSO) and Composite Triple Beat (CTB) values worsen by 2 dB for every 1 dB-increased C/N. The return path laser immediately enters a nonlinear mode called *clipping*, and all communication becomes unreliable. Many return lasers send short bursts above the clipping thresholds and fail on longer or successive bursts.

You should not adjust your input power level by more than 5 dB in a 30-second interval. If you increase the power level by more than 5 dB within 30 seconds, cable interface service on your network is disrupted. If you decrease the power level by more than 5 dB within 30 seconds, cable interfaces on your network are forced offline.

Note When you run the **cable upstream 0 power-level** command, Cisco recommends that the adjacent channel not have a large variation. The recommended maximum input power variance is 5 to 6 dBmV.

To set the upstream input power level in dBmV, use the following command in cable interface configuration mode. The default is 0 dBmV.

```
Router(config-if)# cable upstream usport power-level dbmv
```

## Verifying the Upstream Input Power Level

To verify the current value of the upstream input power level, enter the **show controllers cable** command for the upstream port you have just configured:

```
Router# show controllers cable5/0 u0
Cable5/0 Upstream 0 is up
  Frequency 24.016 MHz, Channel Width 0.800 MHz, QPSK Symbol Rate 0.640 Msps
  Spectrum Group is overridden
  SNR 33.2560 dB
  Nominal Input Power Level 0 dBmV, Tx Timing Offset 2288
  Ranging Backoff automatic (Start 0, End 3)
  Ranging Insertion Interval automatic (60 ms)
  Tx Backoff Start 0, Tx Backoff End 4
  Modulation Profile Group 1
```

Perform these steps if you are having difficulty with verification:

1. Verify that the upstream amplitude of an optimal RF carrier (injected at the fiber node reference input point) reaches the cable interface line card input point at a consistent level (node-to-node and port-to-port).
2. Verify that this absolute level, as installed, matches both the design and software settings on the Cisco uBR7200 series CMTS.

Note Software adjustments of 1 to 3 dB can be used to adjust for minor variations in measurement or setup and port-to-port calibration differences. These adjustments can significantly improve cable interface performance, especially in marginal situations. Larger adjustments should be made in conjunction with spectrum analyzer support at the headend or distribution hub.

# Specifying Upstream Minislot Size

To specify the minislot size (in ticks) for specific upstream cable interfaces, use the following command in cable interface configuration mode. Acceptable values are 2, 4, 8, 16, 32, 64, and 128. The default is 8.

```
Router(config-if)# cable upstream usport minislot-size size
```

For additional information about channel width and minislot size, refer to the *Cable Radio Frequency (RF) FAQs* on Cisco.com.

## Verifying Upstream Minislot Size

To verify upstream minislot size, enter the **show controllers cable** command for the upstream port you have just configured:

```
Router# show controllers cable5/0 u0
Cable5/0 Upstream 0 is up
Frequency 24.016 MHz, Channel Width 1.600 MHz, QPSK Symbol Rate 1.280 Msps
  Spectrum Group is overridden
  SNR 33.2560 dB
  Nominal Input Power Level 0 dBmV, Tx Timing Offset 2288
  Ranging Backoff automatic (Start 0, End 3)
  Ranging Insertion Interval automatic (60 ms)
  Tx Backoff Start 0, Tx Backoff End 4
  Modulation Profile Group 1
  part_id=0xFFFF, rev_id=0xFF, rev2_id=0xFF
  nb_agc_thr=0x0000, nb_agc_nom=0x0000
  Range Load Reg Size=0x58
  Request Load Reg Size=0x0E
  Minislot Size in number of Timebase Ticks is = 8
  Minislot Size in Symbols = 64
  Bandwidth Requests = 0xFE
  Piggyback Requests = 0xD
  Invalid BW Requests= 0x2
  Minislots Requested= 0x2963
  Minislots Granted  = 0x2963
  Minislot Size in Bytes = 16
  Map Advance = 4000 usecs
  UCD Count = 32964
  DES Ctrl Reg#0 = C000C043, Reg#1 = 0
```

Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected.

Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.

Step 3 Ensure that the captive installation screws are tight.

Step 4 Verify that you have entered the correct slot and port numbers.

Step 5 Verify that you selected a valid frequency for your router.

# Setting Upstream Traffic Shaping

Upstream traffic shaping, available on the DOCSIS upstream channel, delays the scheduling of the upstream packet, which in turn causes the packet to be buffered on the cable customer premises equipment (CPE) device, instead of being dropped. This allows the user's TCP/IP stack to pace the application traffic appropriately and approach throughput commensurate with the subscriber's defined quality of service (QoS) levels.

The CMs are buffered without incurring TCP-related timeouts and retransmits. This enables the CMTS to enforce the peak upstream rate for each CM, without degrading overall TCP performance for the subscriber CPEs. Upstream grant shaping is per cable interface (per service ID (SID)).

Token-bucket policing with shaping is the per-upstream default rate-limiting setting at the CMTS. Shaping can be enabled or disabled for the token-bucket algorithm.

To enable upstream traffic shaping for an upstream port on a Cisco cable interface line card, use one of the following commands in cable interface configuration mode.

| | Command | Purpose |
|---|---|---|
| Step 1 | `Router(config-if)# cable upstream` *usport* `rate-limit` | Enables traffic shaping for the specified upstream cable interface. |
| | `Router(config-if)# cable upstream` *usport* `rate-limit token-bucket` | Enables traffic shaping for the upstream cable interface employing the token-bucket policing algorithm. With this command the Cisco uBR7200 series CMTS automatically drops packets in violation of allowable upstream bandwidth. |
| | `Router(config-if)# cable upstream` *usport* `rate-limit token-bucket shaping` | Default. Enables traffic shaping for the upstream cable interface employing the token-bucket policing algorithm with traffic shaping. |
| Step 2 | `Router(config-if)# ^Z`<br>`Router#` | Exits back to the EXEC mode so that you can verify upstream traffic shaping. |

To disable upstream traffic shaping for an upstream port, enter the following command in cable interface configuration mode:

```
Router(config-if)# no cable upstream usport rate-limit
```

The software supports:

- Generic calendar queuing routines
- New token-bucket policing function
- Grant shaping application of the calendar queues
- Upstream rate-shaping option to the **token-bucket** keyword
- A default state change from 1-second burst policing to token bucket with shaping

Tip Upstream grant shaping is per CM (per service ID (SID)). Shaping can be enabled or disabled for the token-bucket algorithm.

Note Before the introduction of this feature, the CMTS would drop bandwidth requests from a CM it detected as exceeding its configured peak upstream rate. Such request dropping affects the throughput performance of IP-based protocols such as FTP, TCP, and Simple Network Management Protocol (SNMP). With this feature, the CMTS can shape (buffer) the grants for a CM that is exceeding its upstream rate, rather than dropping the bandwidth requests.

```
Router# show interface c5/0 sid 1 counters
00:02:23: %ENVM-3-LASTENV: Cannot save environmental data
Sid  Req-polls  BW-reqs    Grants     Packets    Frag       Concatpkts
     issued     received   issued     received   complete   received
1    0          22         22         22         0          0
2    0          3          3          2          0          0
3    0          0          0          0          0          0
```

## Verifying Upstream Traffic Shaping

To determine if upstream traffic shaping is configured and activated, enter the **show running-config** command and look for the cable interface configuration information. If upstream traffic shaping is configured and enabled, a traffic shaping entry appears in the **show running-config** output. If upstream traffic shaping is disabled, **no cable upstream rate-limit** appears in the output.

You can also perform the following tasks to verify that traffic shaping is enabled on the upstream channel:

Step 1 Configure a low-peak upstream rate limit for the CM in its QoS profile. Either use the command-line interface (CLI) to modify the modem's QoS profile, or edit the modem's TFTP configuration file. refer to the*DOCSIS 1.1 for the Cisco uBR7200 Series Universal Broadband Routers* feature module on Cisco.com.

Step 2 Use a regular rate-limiting algorithm on the upstream without rate shaping, and note the drops of the excess bandwidth requests from this CM when it exceeds its peak upstream rate.

Use the **show interface c*x*/*y* sid counters verbose** command to see the bandwidth request drops. Verify that the upstream rate received by that modem is less than its configured peak rate, due to the timeouts and backoffs produced by the drop in bandwidth requests. Enter the **show interface c*x*/*y* service flow qos** command to see the input rate at CMTS in bps.

Step 3 Enable grant shaping on the upstream channel by using the new **shaping** keyword extension to the token-bucket algorithm CLI command.

Step 4 Make the CM exceed its peak upstream rate by generating upstream traffic, and note the effect of grant buffering (shaping) at the CMTS. If you use CM-to-CMTS pings, there is a perceivable decrease in the frequency of the pings.

Let the pings run long enough to allow the averages at the CMTS to settle; then view the upstream rate received by this single modem. Use the **show interface c*x*/*y*** command and see the input rate in bps. This value should be close to the modem's peak upstream rate. Also note the drop counts for the modem's SID by using the **show interface sid counters** command, and verify that the CMTS no longer drops the bandwidth requests from the CM.

The bandwidth request drop count (from the previous nonshaping test) remains unchanged when upstream rate shaping is used, indicating that the CMTS is actually shaping (buffering) the grants for the modem. Verify that the input rate at the CMTS (from the single rate-exceeded CM) stabilizes close to the configured peak rate of 128 Kbps.

## Troubleshooting Tips

Perform these steps if you are having difficulty with verification:

Step 1 Ensure that the cable connections are not loose or disconnected.

Step 2 Ensure that the cable interface line card is firmly seated in its chassis slot.

Step 3 Ensure that the captive installation screws are tight.

Step 4 Verify that you have entered the correct slot and port numbers.

Step 5 Verify that you selected a valid frequency for your router.

# Configuring Optional Cable Modem Interface Features

This section builds on the required CM interface features documented earlier in this chapter. This section provides instructions for several optional CM interface configurations. These interface features pertain to heightened performance and security measures.

Note Default settings are typically adequate to configure optional features on the system. Change default settings only with careful prior analysis.

| Section | Purpose |
|---|---|
| "Activating Host-to-Host Communication (Proxy ARP)" section on page 3-28 | Allows the Cisco uBR7200 series CMTS to issue cable Address Resolution Protocol (ARP) requests on behalf of CMs on the same cable network subnet. |
| "Activating Packet Intercept Capabilities" section on page 3-29 | Specifies a MAC address on the cable network for which interception capabilities are to be activated. |

## Activating Host-to-Host Communication (Proxy ARP)

Cable proxy ARP allows the Cisco uBR7200 series CMTS to issue cable ARP requests on behalf of CMs on the same cable network subnet.

Note Because the downstream and upstreams are separate interfaces, modems cannot directly perform ARP with other modems on the cable plant.

Note The default values for the commands used in this configuration task are adequate in most cases to configure the Cisco uBR7200 series CMTS.

### Activating Cable Proxy ARP Requests

To activate cable proxy ARP for host-to-host communications, use the following command in cable interface configuration mode.

| Command | Purpose |
|---|---|
| `Router(config-if)# cable proxy-arp` | Enables proxy ARP on the cable interface. This is the default. |

#### Verifying Cable Proxy ARP Requests

To verify if cable proxy ARP has been activated or deactivated, enter the **more system:running-config** command and look for the cable interface configuration information. If cable proxy ARP has been activated, it does not appear in the output. If cable proxy ARP has been deactivated, it appears in the output as `no cable proxy-arp`.

```
Router# more system:running-config
Building configuration...

Current configuration:
!
interface cable5/0

 ip address 1.1.1.1 255.255.255.0
 no keepalive
```

```
no cable proxy-arp
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream symbol-rate 5056941
cable upstream 0 frequency 15008000
no cable upstream 0 shutdown
```

Tip If you are having difficulty with verification, make sure that you entered the correct port and cable interface line card slot number when you activated cable proxy ARP.

## Activating Packet Intercept Capabilities

To activate packet intercept functionality, use the following commands in cable interface configuration mode.

| Command | Purpose |
|---|---|
| `Router(config-if)# **cable intercept** *xxxx.xxxx.xxxx*` | Specifies a MAC address on the cable network for which interception capabilities are to be activated. There is a limit of 10 MACs. |
| `Router(config-if)# **no cable intercept** *xxxx.xxxx.xxxx*` | Disables interception after it is enabled. |

# Configuring Cable Subinterfaces

The command to create a subinterface over a cable interface is the same as that defined by Cisco IOS for other software applications:

**interface cable** *x/y.n*

where *x* is the slot number, *y* is the port number, and *n* is the subinterface number.

Each created subinterface is assigned a software IDB. The layer 3 packet arriving over a physical cable interface must be assigned an appropriate software IDB to which it belongs. Since each packet that is received over a cable interface is prepended with its associated SID, this can be extracted from the packet and used as the key to find the associated software IDB. The defined cmts_sid_instance_t structure holds information pertaining to the SID and is extended to include the associated software IDB pointer.

The IP address stored in the DHCP reply is matched for its subnet value against the subnet value configured for each of the subinterfaces over the physical cable interface. The subnet information is derived by combining the IP address and the mask value available in the software IDB structure.

The linked list of software IDBs can be accessed from the hardware IDB associated with the physical cable interface. At the time of CM registration, the software IDB address is initialized to null as the mapping is unknown at first.

Tip In current releases of software, the SID-to-subinterface mapping is done based on the DHCP-assigned IP address and is not user configurable.

### Subinterface Configuration Example

The following example shows how to define a subinterface on the cable5/0:

```
interface cable5/0
! No IP address
! MAC level configuration only
```

```
! first subinterface
interface cable5/0.1
description Management Subinterface
ip address 10.255.1.1 255.255.255.0
cable helper-address 10.151.129.2

! second subinterface
interface cable5/0.2
ip address 10.279.4.2 255.255.255.0
cable helper-address 10.151.129.2

! third subinterface
interface cable5/0.3
ip address 10.254.5.2 255.255.255.0
cable helper-address 10.151.129.2
```

### Subinterface Definition on Bundle Master Example

The following example shows how to define subinterfaces on a bundle master and define Layer 3 configurations for each subinterface. In this example, the interfaces `int c5/0` and `int c4/0` are bundled.

```
int c5/0
! No IP address
! MAC level configuration only
cable bundle 1 master

int c4/0
! No IP address
! MAC layer configuration
cable bundle 1

! first subinterface
int c5/0.1
ip address 10.22.64.0 255.255.255.0
cable helper-address 10.4.1.2

! second subinterface
int c5/0.2
ip address 10.12.39.0 255.255.255.0
cable helper-address 10.4.1.2

! third subinterface
int c5/0.3
ip address 10.96.3.0 255.255.255.0
cable helper-address 10.4.1.2
```

## Configuring and Monitoring Cable Interface Bundling

Cable interface bundling allows you to reduce the number of subnets consumed per Cisco uBR7200 series. Multiple cable interfaces can share a single IP subnet. An IP subnet is required for each bundle. You can bundle all cable interfaces on a Cisco uBR7200 series into a single bundle.

Using the CLI, first configure a master interface for a cable interface bundle. The master interface has an IP address assigned and is visible for IP routing functionality. After you configure the master interface, add additional cable interfaces to the same interface bundle. Those interfaces must not have an IP address assigned. You can also configure multiple bundle interfaces.

You can configure up to four interface bundles. In each bundle, specify exactly one interface as the master interface, using the "master" keyword. In the case of a subinterface over a cable bundle, `x' is the interface number of the bundle master [1]. The subinterface number starts from 1.

Caution Configure an IP address on the master interface only. An attempt to add an interface to a bundle will be rejected if an IP address is configured and the interface is not specified as a master interface.

When bundling cable interfaces, only the interface configured to be the bundle master is allowed to have subinterfaces. An interface that has subinterface(s) defined over it will not be allowed to be part of a bundle.

MIB objects on cable interface bundles are not supported as of the date of this publication.

Tip Generic cable interface configuration such as source verify or ARP handling will apply to subinterfaces as well.

Note If a physical interface goes down, the associated subinterface will also go down. If the subinterface is defined over the cable bundle and the bundle master is shut down or removed, no data packets will be sent to any of the subinterfaces defined over it. Packets will still be received from non-master interfaces, but will be dropped.

## Using Interface Bundling Commands

Use the following commands to configure and view cable interface bundles in privileged EXEC mode:

| Command | Purpose |
|---|---|
| `Router(config-if)# cable bundle` *n* `master` | Configures the interface **n** to be the master interface in a bundle. Valid range is 1 to 255. |
| `Router# show cable bundle` *n* `forwarding-table` | Displays the forwarding table for the specified interface. |

## Configuration Guidelines

Use the **cable bundle** interface configuration command to configure a cable interface to belong to a bundle. Specify the bundle identifier—1 to 255. Optionally define the specified interface as the master.

Specify IP networking information, including IP address, routing protocols, and switching modes, on the bundle master. Do not specify generic IP networking information on bundle slave interfaces.

If you attempt to add an interface to a bundle as non-master interface and an IP address is assigned to this interface, the command will fail. You must remove the IP address configuration before you can add the interface to a bundle.If you have configured an IP address on a bundled interface and the interface is not the master interface, a warning message appears.

Specify generic (that is, not downstream or upstream related) cable interface configurations, such as source-verify or ARP handling, on the master interface. Do not specify generic configuration on non-master interfaces.

If you configure an interface as part of a bundle and it is not the master interface, all generic cable configuration for this interface is removed. The master interface configuration will then apply to all interfaces in the bundle.

If you shut down or remove the master interface in a bundle, no data packets are sent to any of the interfaces in this bundle. Packets will still be physically received from non-master interfaces which have not been shut down, but those packets will be discarded. This means that cable modems connected to those interfaces will not be disconnected immediately, but CMs coming online will not be able to obtain an IP address, download their DOCSIS configuration file, or renew their IP address assignment if the DHCP lease expires.

If you shut down a slave interface, only the specific interface is affected.

## Cable Interface Bundling Examples

In the following configuration example, interface 25 is configured as the master interface in the bundle:

```
Router(config-if)# cable bundle ?
<1-255>  Bundle number
Router(config-if)# cable bundle 25 ?
master  Bundle master
  <cr>
Router(config-if)# cable bundle 25 master ?
<cr>
Router(config-if)# cable bundle 25 master
Router(config-if)#
07:28:17: %UBR7200-5-UPDOWN: Interface Cable3/0 Port U0, changed state to down
07:28:18: %UBR7200-5-UPDOWN: Interface Cable3/0 Port U0, changed state to up
Router# show cable bundle 25 forwarding-table
MAC address         Interface
0050.7366.17ab      Cable3/0
0050.7366.1803      Cable3/0
0050.7366.1801      Cable3/0
```

The following example shows an error message you receive if you try to configure an interface with an IP address that is not the master interface:

```
Router(config-if)# cable bundle 5
Please remove ip address config first then reenter this command
```

To display the forwarding table for a specified interface, use the **show cable bundle** command in privileged EXEC mode. A sample is shown below:

```
Router# show cable bundle 25 forwarding-table

MAC address         Interface
0050.7366.17ab      Cable3/0
0050.7366.1803      Cable3/0
0050.7366.1801      Cable3/0
```

The following example shows how to bundle a group of physical interfaces. In this example, the interfaces `int c5/0` and `int c4/0` are bundled.

```
int c5/0
ip address 209.165.200.225 255.255.255.0
ip address 209.165.201.1 255.255.255.0 secondary
cable helper-address 10.5.1.5
! MAC level configuration
cable bundle 1 master
int c4/0
! No IP address
! MAC layer configuration only
cable bundle 1
```

The following example shows how to configure interface 25 to be the master interface:

```
Router(config-if)# cable bundle 25 master
Router(config-if)#
07:28:17: %UBR7200-5-UPDOWN: Interface Cable3/0 Port U0, changed state to down
07:28:18: %UBR7200-5-UPDOWN: Interface Cable3/0 Port U0, changed state to up
```

The following example shows the error message you get if you try to configure an interface with an IP address that is not the master interface:

```
Router(config-if)# cable bundle 5
Please remove ip address config first then reenter this command
Router(config-if)#
```

# Configuring Payload Header Suppression and Restoration

Payload Header Suppression (PHS) is a new feature in the DOCSIS1.1 MAC driver. The PHS feature is used to suppress repetitive or redundant portions in packet headers before transmission on the DOCSIS link. The upstream receive driver is now capable of restoring headers suppressed by CMs, and the downstream driver is capable of suppressing specific fields in the packet header before forwarding the frame to the CM.

| Command | Purpose |
|---|---|
| **show interface cable** *x/0* **service-flow [***sfid***] phs** | Displays cable interface information. |
| **debug cable error** | Displays errors that occur in the cable MAC protocols. To disable debugging output, use the **no** form of the command. |
| **debug cable phs** | Displays the activities of the PHS and restoration driver. The **no** form of this command disables debugging output. |

# Setting Optional IP Parameters (Broadcast and Multicast Echo)

You can set additional IP parameters to enable downstream echoing of upstream data. This section contains two procedures to configure these optional IP parameters:

- "Activating IP Multicast Echo" section on page 3-33
- "Activating IP Broadcast Echo" section on page 3-34

Note The default values for the commands used in these configuration steps are adequate in most cases to configure the Cisco uBR7200 series CMTS.

## Activating IP Multicast Echo

The Cisco uBR7200 series CMTS echos IP multicast packets by default. To activate IP multicast echo if it has been previously disabled, use the following command in cable interface configuration mode.

| Command | Purpose |
|---|---|
| `Router(config-if)#` **cable ip-multicast-echo** | Enables IP multicast echo. This is the default. |

To disable IP multicast echo, enter the **no cable ip-multicast-echo** command in cable interface configuration mode.

## Verifying IP Multicast Echo

To determine whether IP multicast echo is activated or deactivated, enter the **more system:running-config** command, and look for the cable interface configuration information. If IP multicast echo is activated, there is no notation in the output, because this is the default setting. If IP multicast echo is deactivated, a notation appears in the output:

```
Router# more system:running-config
Building configuration...

Current configuration:
!
interface cable5/0

 ip address 1.1.1.1 255.255.255.0
 no keepalive
 no cable ip-multicast-echo
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable upstream 0 frequency 15008000
 no cable upstream 0 shutdown
```

Tip If you are having difficulty with verification, make sure that you entered the correct slot and port numbers when you entered cable interface configuration mode.

# Activating IP Broadcast Echo

By default, the Cisco uBR7200 series CMTS does not echo IP broadcast packets. To activate IP broadcast echo, use the following command in cable interface configuration mode.

| Command | Purpose |
|---|---|
| `Router(config-if)# cable ip-broadcast-echo` | Enables IP broadcast echo. |

To disable IP broadcast echo when it is enabled, enter the **no cable ip-broadcast-echo** command in cable interface configuration mode.

## Verifying IP Broadcast Echo

To determine whether IP broadcast echo is activated or deactivated, enter the **more system:running-config** command and look for a notation in the cable interface configuration information:

```
Router# more system:running-config
Building configuration...

Current configuration:
!
interface cable5/0

 ip address 1.1.1.1 255.255.255.0
 no keepalive
 cable ip-broadcast-echo
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable upstream 0 frequency 15008000
 no cable upstream 0 shutdown
```

# Configuring DOCSIS Baseline Privacy Interface on the Cisco uBR7200 Series

This chapter describes the DOCSIS 1.0 Baseline Privacy Interface (BPI), guidelines for configuring DOCSIS BPI on the Cisco uBR7200 series, and features of DOCSIS 1.1 Baseline Privacy Interface Plus (BPI+). This chapter contains the following sections:

| Section | Description |
|---|---|
| "Baseline Privacy Interface Overview" section on page 4-1 | Provides a description of DOCSIS 1.0 BPI, BPI key management, CM cummunication with the BPI, and illustrations. |
| "Enabling DOCSIS BPI" section on page 4-3 | Provides guidelines for enabling DOCSIS 1.0 BPI on the Cisco uBR7200 series. |
| "DOCSIS 1.1 Baseline Privacy Interface Plus Overview" section on page 4-4 | Provides an overview of the features in DOCSIS 1.1 BPI+. |

## Baseline Privacy Interface Overview

Baseline Privacy Interface (BPI) is defined as a set of extended services within the DOCSIS MAC sublayer. BPI gives subscribers data privacy across the RF network, encrypting traffic flows between the CMTS and CM.

Note Encryption/decryption is subject to export licensing controls.

The level of data privacy is roughly equivalent to that provided by dedicated line network access services such as analog modems or digital subscriber lines (DSL). BPI provides basic protection of service, ensuring that a CM, uniquely identified by its MAC address, can obtain keying material for services only it is authorized to access.

Note Because DOCSIS 1.0 BPI does not authenticate CMs, it does not protect against users employing cloned CMs masquerading as authorized CMs. Specific Cisco IOS releases provide protection against spoofing, and provide supporting commands that can be used to configure source IP filtering on RF subnets to prevent a user from using a source IP address that is not valid for the connected IP subnet.

BPI extends the definition of the MAC sublayer's SID. The *DOCSIS RF Interface Specification* (viewable at http://www.cablemodem.com/specifications.html) defines a SID as a mapping between CMTS and CM to allocate upstream bandwidth and class of service management. When BPI is activated, the SID also identifies a particular security association and has upstream and downstream significance.

When BPI is operational, downstream multicast traffic flow that typically does not have a SID associated with it, now has a SID. The Privacy Extended Header Element includes the SID associated with the MAC Packet Data Physical Data Unit (PDU). The SID along with other components of the extended header element identifies to a CM the keying material required to decrypt the MAC PDU's packet data field.

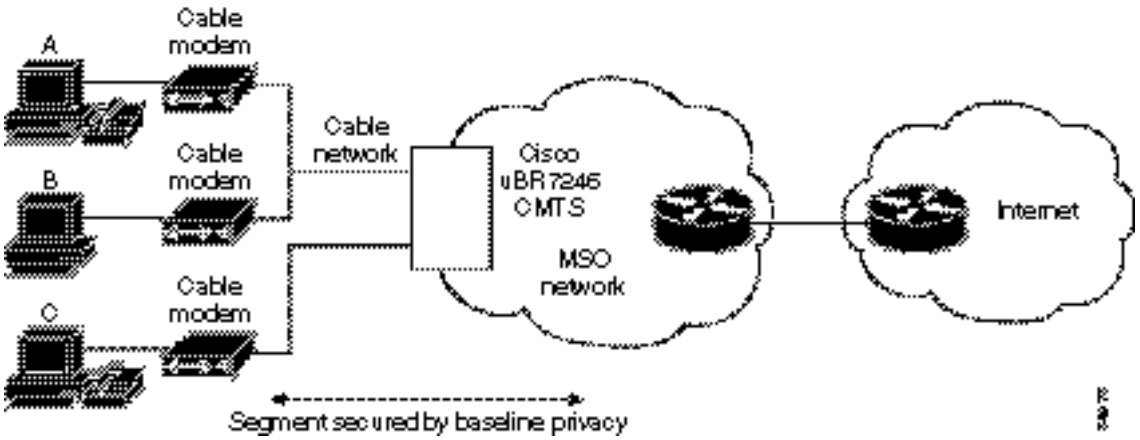
BPI's key management protocol runs between the CMTS and the CM. CMs use the protocol to obtain authorization and traffic keying material relevant to a particular SID from the CMTS and to support periodic reauthorization and key refresh.

The key management protocol uses RSA—a public key encryption algorithm—and the electronic codebook (ECB) mode of DES to secure key exchanges between the CMTS and a CM. Privacy is in the form of 56-bit (the default) or 40-bit encryption between the CMTS and CM. Since BPI is part of DOCSIS, all DOCSIS-certified CMs and qualified CMTS are fully interoperable. Figure 4-1shows a BPI architecture.

Note CMs must have factory-installed RSA private/public key pairs to support internal algorithms to generate key pairs prior to first BPI establishment.

A SID's keying material has a limited life span. When the CMTS delivers SID keying material to a CM, it also provides the CM with the lifetime value.

*Figure 4-1 BPI Network Example*




# BPI Key Management

BPI initialization begins with the CM sending the CMTS an authorization request, containing data identifying:

- CM—48-bit IEEE MAC address
- CM's RSA public key
- List of zero or more assigned unicast SIDs that have been configured to run BPI

At that time, BPI provides basic protection against theft of service by ensuring the CM, identified by its MAC address, can obtain keying materials only it is authorized to access. The CMTS replies with a list of SIDs on which to run BPI. The reply also includes an authorization key from which the CM and CMTS derive the keys needed to secure a CM's subsequent requests for additional encryption keys. After obtaining the traffic encryption key, the CMs begin to transmit encrypted data.

## Differentiating Traffic Streams

BPI only encrypts data on the cable network and only encrypts the user data itself, not cable MAC headers. BPI also does not encrypt MAC management messages. After BPI is enabled, however, and encryption has been negotiated for a given SID, all user data sent via that SID is encrypted. BPI differentiates traffic based on SID alone.

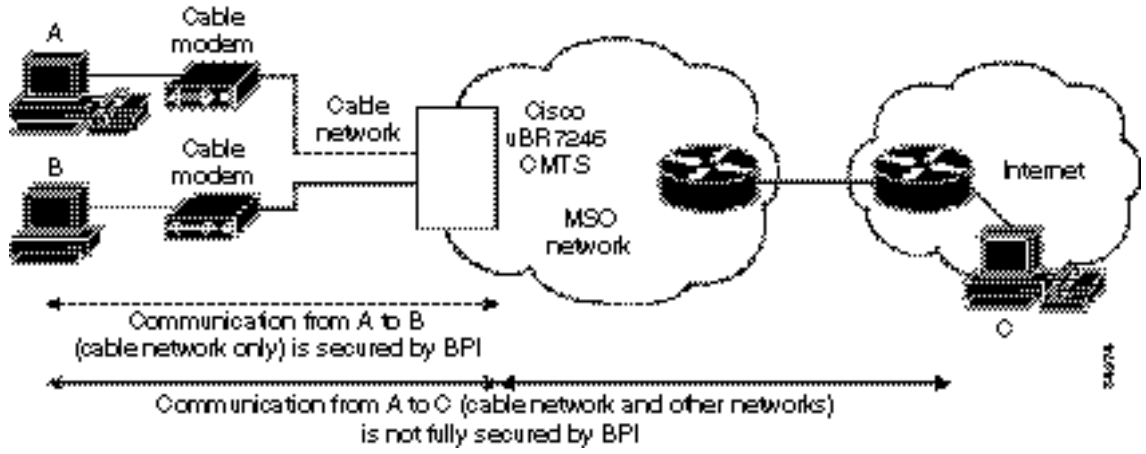
## CM Communication with BPI

Figure 4-2 illustrates BPI communications. When user A sends packets to user B, the CM encrypts those packets using special keys specific to user's A CM. Packets are then transmitted to the CMTS where they are decrypted.

If user B is attached to the cable TV network, the CMTS then re-encrypts the information using a key specific to user B and the encrypted data is passed to user B's CM where it is decrypted and sent to user B. In this manner, an unauthorized user is not able to see unencrypted traffic between user A and user B.

Caution Since BPI occurs only on the cable TV network, however, all traffic going upstream will be decrypted as it passes the CMTS. If user A is attempting to communicate with someone beyond the cable network—user C—all traffic beyond the CMTS will not be encrypted.

*Figure 4-2 BPI Encrypted Data on the Cable TV network*




# Enabling DOCSIS BPI

To enable BPI, choose software images at both the CMTS and CM that support the mode of operation. For the Cisco uBR7200 series software, choose an image with "k1" in its file name or BPI in the feature set description. For Cisco uBR924 cable access routers, all CM images from Cisco IOS Release 12.0(5)T1 or later support this by default. For earlier Cisco IOS release cable modem images, choose an image with "k1" in its file name or BPI in the feature set description.

Note For the CMTS, BPI is enabled by default when you select an image that supports BPI. For CMs, enable BPI via the DOCSIS configuration file using one of the provisioning tools identified in the "DOCSIS 1.0 Feature Support" section on page 1-49.

When baseline privacy is enabled, the Cisco uBR7200 series generates Traffic Encryption Keys (TEKs) for each applicable SID; 56-bit encryption/decryption is the default for Cisco uBR7200 series equipment.

The router uses the keys to encrypt downstream data and decrypt upstream traffic from two-way cable interfaces. The Cisco uBR7200 series router generates keys for unicast, broadcast, and multicast operation as appropriate. Keys are refreshed periodically and have a default lifetime of 12 hours.

# DOCSIS 1.1 Baseline Privacy Interface Plus Overview

DOCSIS 1.0 included a BPI to protect user data privacy across the shared-medium cable network and to prevent unauthorized access to DOCSIS-based data transport services across the cable network. BPI encrypts traffic across the RF interface between the cable modem and CMTS, and also includes authentication, authorization, and accounting (AAA) features.

BPI supports access control lists (ACLs), tunnels, filtering, protection against spoofing, and commands to configure source IP filtering on RF subnets to prevent subscribers from using source IP addresses that are not valid.

DOCSIS 1.1 enhances these security features with Baseline Privacy Interface Plus (BPI+), which includes the following enhancements:

- Digital certificates provide secure user identification and authentication.
- Key encryption uses 168-bit Triple DES (3DES) encryption that is suitable for the most sensitive applications.
- 1024-bit public key with Pkcs#1 Version 2.0 encryption.
- Multicast support.
- Secure software download allows a service provider to upgrade a cable modem's software remotely, without the threat of interception, interference, or alteration.

Note BPI+ is described in the *Baseline Privacy Interface Plus Specification* (SP-BPI+-I07-010829), available from CableLabs (http://www.cablelabs.com).

# Managing Cable Modems on the Hybrid Fiber-Coaxial Network

After you have completed upstream and downstream configuration in Chapter 2, "Configuring the Cable Modem Termination System for the First Time,"you have additional options to manage how your cable modems (CMs) operate in the hybrid fiber-coaxial (HFC) network. You can set the following CM functions:

| Section | Purpose |
|---|---|
| "Activating Cable Modem Authentication" section on page 5-2 | Provides instructions to require all CMs to return a known text string to register with the CMTS and gain access to the network. |
| "Activating Cable Modem Insertion Interval" section on page 5-3 | Limits the amount of time that a CM requests a channel for the first time from the Cisco uBR7200 series. |
| "Activating Cable Modem Upstream Address Verification" section on page 5-4 | Ensures that only CMs that have received DHCP leases through the Cisco uBR7200 series CMTS can access the HFC network. |
| "Clearing Cable Modem Counters" section on page 5-5 | Clears the counters for the CMs in the station maintenance list. |
| "Clearing Cable Modem Reset" section on page 5-5 | Removes one or more CMs from the station maintenance list and resets the cable modem (or all CMs) on the network. |
| "Configuring Cable Modem Registration Timeout" section on page 5-6 | Specifies the registration timeout interval for CMs connected to the Cisco uBR7200 series CMTS. |
| "Configuring Dynamic Contention Algorithms (Cable Insertion Interval, Range, and Data Backoff)" section on page 5-6 | Configures the algorithms that control the capacity of the contention subchannel and how efficiently a given contention subchannel capacity is used. |
| "Configuring the Dynamic Map Advance Algorithm" section on page 5-7 | Enhances the upstream throughput from a CM connected to the Cisco uBR7200 series CMTS. The system employs a new algorithm that automatically tunes the lookahead time in MAC allocation and management messages (MAPs), based on several input parameters for the corresponding upstream channel. |
| "Configuring Maximum Hosts Attached to a Cable Modem" section on page 5-8 | Specifies the maximum number of hosts that can be attached to a subscriber's CM. |
| "Configuring Per-Modem Filters" section on page 5-8 | Provides instructions to configure the Cisco uBR7200 series to filter incoming packets from individual hosts or cable interfaces based on the source Media Access Controller (MAC) or Internet Protocol (IP) address. |
| "Configuring Sync Message Interval" section on page 5-9 | Specifies the sync message interval between successive sync message transmissions from the Cisco uBR7200 series CMTS. |

Note Cisco recommends using default values for most commands. The default values for the commands used in these configuration steps are, in most cases, adequate to configure the Cisco uBR7200 series.

For information about setting rate limiting on CMs, refer to these sections in Chapter 3:

- "Setting Downstream Traffic Shaping" section on page 3-10
- "Setting Upstream Traffic Shaping" section on page 3-26

# Activating Cable Modem Authentication

The Cisco uBR7200 series router can be configured to require all CMs to return a known text string to register with the CMTS and gain access to the network. The text string can be from 1 to 80 characters in length. The default setting is "on" (CM authentication is activated).

To activate CM authentication, use the following command in cable interface configuration mode:

| Command | Purpose |
|---|---|
| **cable shared-secret** [*0*\|*7*] **authorization-key** | Enables CM authentication:<br>• *0* specifies an unencrypted authentication key.<br>• *7* specifies an encrypted authentication key. |
| **no cable shared-secret** | Disables CM authentication. |

Tip Ensure that you enter the correct slot and port number, and verify that the cable interface configuration file contains a matching key.

Note The Cisco uBR7200 series router will accept any DOCSIS configuration file with any shared secret if the CMTS configuration does not contain a setting for shared secret. However, if the CMTS configuration contains a setting for shared secret, the settings between the DOCSIS configuration file and the CMTS configuration must match. The shared secret for the CMTS configuration must be entered again or the file will no longer contain the correct MD-5 MIC setting, and CMs will stop working, registering in state reject(m).

## Verifying CM Authentication

To verify if CM authentication has been activated or deactivated, enter the **more system:running-config** command and look for the cable interface configuration information. If CM authentication has been activated, it does not appear in this output. If CM authentication has been deactivated, it appears in this output as "`no cable secret-shared`," as shown in this sample command output:

```
Router# more system:running-config
Building configuration...
Current configuration:
!
interface Cable5/0
 ip address 1.1.1.1 255.255.255.0
 no keepalive
```

```
 no cable secret-shared
 cable insertion-interval 150000
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream symbol-rate 5056941
cable upstream 0 frequency 15008000
cable upstream 0 fec
cable upstream 0 scrambler
no cable upstream 0 shutdown
!
```

### Troubleshooting CM Authentication

If you are having trouble, make sure that you entered the correct slot and port numbers when you entered cable interface configuration mode. For additional troubleshooting information, refer to Chapter 8, "Troubleshooting the System."

## Activating Cable Modem Insertion Interval

When a CM is ready to transmit data, it requests a channel from the Cisco uBR7200 series. You can limit the amount of time that a CM requests a channel for the first time from the Cisco uBR7200 series. A CM's initial channel request is known as *insertion*. The valid range is 100 to 2000 milliseconds.

To activate the CM insertion interval, use the following command in cable interface configuration mode.

| Command | Purpose |
|---|---|
| **cable insertion-interval** ***milliseconds*** | Sets the insertion interval in milliseconds. |

### Validating Cable Modem Insertion Interval

To verify that a CM insertion interval has been set, enter the **more system:running-config** command, and look for the cable interface configuration information, as shown in this sample command output:

```
Router# more system:running-config
Building configuration...
Current configuration:
!
interface Cable5/0
 ip address 1.1.1.1 255.255.255.0
 no keepalive
 cable insertion-interval 2000
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream symbol-rate 5056941
 cable upstream 0 frequency 15008000
 cable upstream 0 fec
 cable upstream 0 scrambler
 no cable upstream 0 shutdown
!
```

### Troubleshooting Cable Modem Insertion Interval

If you are having trouble, make sure that you entered the correct slot and port numbers when you typed the command.

# Activating Cable Modem Upstream Address Verification

CM upstream address verification ensures that only CMs that have received Dynamic Host Configuration Protocol (DHCP) leases through the Cisco uBR7200 series CMTS can access the HFC network. The Cisco uBR7200 series CMTS discards all packets received from or for hosts that have not received Dynamic Host Configuration Protocol (DHCP)-assigned addresses. The default setting is "off" (CM upstream address verification is deactivated).

To activate or deactivate CM upstream verification, use the following command in the cable interface configuration mode:

| Command | Purpose |
|---|---|
| **cable source-verify** [**dhcp**] | Activates CM upstream verification. The **dhcp** option specifies that queries be sent to verify unknown IP addresses in upstream data packets. |
| **no cable source-verify** | Returns to the default upstream verification state. |

## Verifying Cable Modem Upstream Address Verification

To verify that CM upstream verification has been activated or deactivated, enter the **more system:running-config** command and look for the `no cable source-verify` notation in the cable interface configuration information. If CM upstream verification has been deactivated, it does not appear in this output. If CM upstream verification has been activated, it appears in this output as `cable source-verify`, as shown in this command output excerpt:

```
Router# more system:running-config
Building configuration...
Current configuration:
!
interface Cable5/0
 ip address 1.1.1.1 255.255.255.0
 no keepalive
  cable source-verify
  cable insertion-interval 2000
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream symbol-rate 5056941
 cable upstream 0 frequency 15008000
 cable upstream 0 fec
 cable upstream 0 scrambler
 no cable upstream 0 shutdown
!
```

Tip Be sure that you enter the correct slot and port number when you enter the cable interface configuration mode.

Note If the Cisco uBR7200 series router is reloaded or the Address Resolution Protocol (ARP) table is cleared, all hosts on the network are forced to release and renew their IP addresses. Some systems might require restarting if the IP protocol stack is unable to renew using a broadcast IP address.

# Clearing Cable Modem Counters

To clear the counters for the CMs in the station maintenance list, use one of the following commands in cable interface configuration mode.

| Command | Purpose |
|---|---|
| **clear cable modem** *mac-addr* **counters** | Clears the counters in the station maintenance list for the CM with a specific MAC address. |
| **clear cable modem** *ip-addr* **counters** | Clears the counters in the station maintenance list for the CM with a specific IP address. |
| **clear cable modem all counters** | Clears the counters in the station maintenance list for all CMs. |

## Verifying Clear Cable Modem Counters

To determine if the counters in the station maintenance list are cleared, enter one of the **following** commands. The station maintenance list counter is 0.

| Command | Purpose |
|---|---|
| **show cable modem** *ip-address* | Displays the status of a CM identified by its IP address. |
| **show cable modem** *mac-address* | Displays the status of a CM identified by its MAC address. |
| **show cable modem** *interface-address* | Displays the status of all CMs on a particular upstream. |

# Clearing Cable Modem Reset

To remove one or more CMs from the station maintenance list and reset the cable modem (or all CMs) on the network, use one of the following commands in cable interface configuration mode.

| Command | Purpose |
|---|---|
| **clear cable modem** *mac-addr* **reset** | Removes the CM with a specific MAC address from the station maintenance list and resets it. |
| **clear cable modem** *ip-addr* **reset** | Removes the CM with a specific IP address from the station maintenance list and resets it. |
| **clear cable modem all reset** | Removes all CMs from the station maintenance list and resets them. |

## Verifying Clear Cable Modem Reset

To determine if the **clear cable modem reset** command has removed a CM from the station maintenance list and forced it to start a reset sequence, enter the **show cable modem** command.

Tip Be sure that you entered the correct CM IP address or MAC address when you typed the **clear cable modem reset** command. It might take up to 30 seconds for the CM to start the reset sequence.

Note The **clear cable modem reset** command is useful if a Simple Network Management Protocol (SNMP) manager is not available, or if the CM is unable to obtain an IP address or respond to SNMP messages.

# Configuring Cable Modem Registration Timeout

By default, registered CMs that have no upstream activity for three minutes are timed out and disconnected from the Cisco uBR7200 series CMTS. This timeout interval can be decreased to 2 minutes or increased up to 60 minutes.

To specify the registration timeout interval for CMs connected to the Cisco uBR7200 series CMTS, use the following command in cable interface configuration mode.

| Command | Purpose |
|---|---|
| **cable registration-timeout** *n* | Specifies the maximum number of minutes allowed to elapse with no upstream activity before terminating the connection. Valid range is from 2 to 60 minutes. Default = 3 minutes. |

# Configuring Dynamic Contention Algorithms (Cable Insertion Interval, Range, and Data Backoff)

The Cisco uBR7200 series software includes the following algorithms that control the capacity of the contention subchannel and control the efficient use of a given contention subchannel capacity:

- Algorithm that dynamically controls the rate of upstream contention slots—initial ranging and bandwidth requests.
- Algorithm that varies the backoff parameters that CMs use. Backoff variation falls within each of the initial ranging and bandwidth request upstream contention subchannels.

In high contention mode, the Cisco uBR7200 series MAC scheduler uses collision statistics and sustains a high frequency of initial ranging slots until it detects a steady ranging state. The CMTS dynamically varies the frequency of initial ranging slots using the data grant utilization on the upstream channels. The CMTS trades upstream bandwidth between data grants and initial ranging slots. The CMTS autodetects a high collision state and switches to low insertion interval mode after a steady state is achieved where few collisions occur.

The CMTS is careful when monitoring the ranging channel health to revert to a steady state. In steady state mode, data grants—grant utilization—receive preference over initial ranging slots.

Although the binary exponential backoff algorithm operates in a distributed fashion at different CMs, the CMTS provides centralized control for the backoff algorithm. To achieve this, it remotely monitors traffic load—the backlog developing on the contention channel—and then varies the backoff start and end specified in the MAPs for that upstream channel. This ensures that colliding CMs are properly randomized in time.

The following cable interface commands are available to configure the dynamic contention algorithms:

```
[no] cable insertion-interval [automatic [Imin [Imax]]] | [msecs]
[no] cable upstream port num range-backoff [automatic] | [start end]
[no] cable upstream port num data-backoff [automatic] | [start end]
```

## cable insertion-interval Command Examples

To deviate from system defaults when modifying the dynamic contention algorithm, use one of the following commands in cable interface configuration mode.

| Command | Purpose |
|---|---|
| **[no] cable insertion-interval [automatic [*Imin* [*Imax*]]] \| [*msecs*]** | Enables or disables the dynamic ranging interval algorithm. If lower and upper bounds for varying the period are not specified, the system uses default frequency values of initial ranging upstream slots between 50 milliseconds to 2 seconds, respectively. |
| **cable insertion-interval automatic min 25-2000** | Sets the lower bound on the initial ranging period for the automatic ranging algorithm. |
| cable insertion-interval max 500-2000 | Sets the upper bound on initial ranging period for the automatic ranging algorithm. |
| no cable insertion-interval | Resets fixed initial ranging period to default value of 500 msecs. Also invokes fixed initial ranging algorithm. |
| cable insertion-interval 100-2000 | Enables fixed initial ranging period algorithm with specified fixed period (msecs). |

Tip System defaults are to have dynamic ranging interval enabled, dynamic ranging backoff enabled, and fixed data backoffs for each upstream of a cable interface.

The default **automatic** insertion interval setting enables the Cisco automatic initial ranging period algorithm, where lower and upper default values of 50 msecs and 2 secs are used. The default **automatic range-backoff** setting enables the dynamic backoff algorithm.

# Configuring the Dynamic Map Advance Algorithm

A CMTS administrator can enhance the upstream throughput from a CM connected to the Cisco uBR7200 series CMTS. The system employs a new algorithm that automatically tunes the lookahead time in MAPs, based on several input parameters for the corresponding upstream channel. The use of dynamic and optimal lookahead time in MAPs significantly improves the per-modem upstream throughput.

Caution Only a trained CMTS administrator should adjust these values.

To configure the dynamic map advance algorithm, use the **cable map-advance dynamic** [*n*]|*static* command in cable interface configuration mode.

This command specifies a value to enhance the upstream throughput from a CM connected to the Cisco uBR7200 series router. The *n* argument provides the safety factor for the dynamic map advance algorithm. This argument is specified in usecs and controls the amount of extra lookahead time in MAPs to account for inaccuracies of the measurement system and software latencies. The default value is 1000 usecs.

You can vary this value from 500 to 1500 usecs. This argument is a delta value added to the dynamic **map-advance** setting that the algorithm computes. Using larger safety factors increases the run-time lookahead in MAPs, but reduces the upstream performance.

Use the **static** keyword for the **cable map-advance** command. The Cisco uBR7200 series router uses a fixed lookahead time in MAPs, regardless of the real propagation delay of the farthest CM on the network. This fixed lookahead time is computed based on the worst-case parameters, such as farthest DOCSIS propagation delay for the CMs.

Caution If you are adjusting the dynamic map-advance algorithm, do not reduce the safety factor below the default value of 1000 usecs in a production network, until you are confident that the reduced safety factor suffices for your deployment. The default value is chosen to be a safe operating point for the algorithm.

# Configuring Maximum Hosts Attached to a Cable Modem

To specify the maximum number of hosts that can be attached to a subscriber's CM, use the following command in cable interface configuration mode.

| Command | Purpose |
|---|---|
| **cable max-hosts** *n* | Specifies the maximum number of hosts that can be attached to a CM on this interface. Valid range is from 0 to 255 hosts. Default = 0. |
| **no cable max-hosts** | Resets the allowable number of hosts attached to a CM to the default value of 0 hosts. |

# Configuring Per-Modem Filters

You can configure the Cisco uBR7200 series to filter incoming packets from individual hosts or cable interfaces based on the source Media Access Controller (MAC) or Internet Protocol (IP) address. Definition of filters follows standard Cisco IOS configuration practices for access lists and groups.

Note Configuring per modem or host filters is supported in Cisco IOS Release 12.0(5)T1 or higher, as well as in Cisco IOS Release 12.0(6)SC or higher.

To specify the access group (per-modem filter), use the **cable modem access-group** command in privileged EXEC mode. To disable the specification, use the **no access-group** form of this command.

**cable modem** {*mac-addr* | *ip-addr*} **access-group** [*access-list* | *access-name*]

**cable modem** {*mac-addr* | *ip-addr*} **no access-group**

Syntax Description

| | |
|---|---|
| *ip-addr* | Specifies the IP address for the CM. |
| *mac-address* | Specifies the MAC address for the CM. |
| *access-list* | Specifies the IP access list (standard or extended). Valid values are 1 to 199. |
| *access-name* | Specifies the access-list name. |

Examples

The following example shows the **cable modem access-group** command assigning access-list 1 to the CM with the MAC address of abcd.ef01.2345:

```
Router# cable modem abcd.ef01.2345 access-group 1
```

This command configures access lists to be specified on a per-interface and per-direction basis. The packets received from cable interfaces and/or individual hosts are filtered based on the cable interface or the host the packets are received from. Use *modem* if the device is a CM. Use *host* if the device is a CPE device attached to a CM.

The *macaddr* specifies the CM's or CPE device's unique MAC address. Define the filter to be applied to the device and a given address.

Use the *ipaddr* option to specify the CM or CPE device's current IP address.

Use the *acl* option to assign the CM or CPE device to an access list. This defines the per-CM or per-host filter requirements implemented at the CMTS, rather than at the CM. Access list numbers are 1 to 99 for fast IP access lists, 100 to 199 for show extended IP access lists.

Note Access list numbers of 700 to 799 do not apply.

Caution The system applies filters after the CM registers with the CMTS. Filter definitions are not saved across system reboots and must be applied each time a CM registers.

The software supports traps to alert CMTS administrators on CMs going offline or back online. A typical registration and login procedure is shown below:

1. The CM registers with the Cisco uBR7200 series.
2. The Cisco uBR7200 series sends traps to management systems in use for the network.
3. The management system sets per modem filters using SNMP or *rsh*.
4. The user logs in at the server.
5. The login server obtains required modem and CPE information from the Cisco uBR7200 series.
6. The login server sets per-CPE filter in the Cisco uBR7200 series. The per-CPE filter overrides the per modem filter settings.
7. If the CM goes offline for a brief period of time, filters defined using the Cisco uBR7200 series remain active. If a CM stays offline for more than 24 hours, filter settings are reset.
8. If the user logs out or the login server detects that the user is not online, the login server sets default filters for the CM or the CPE device.

# Configuring Sync Message Interval

To specify the sync message interval between successive sync message transmissions from the Cisco uBR7200 series CMTS, use the following command in cable interface configuration mode.

| Command | Purpose |
|---|---|
| **cable sync-interval** *msec* | Specifies the interval in milliseconds between successive sync message transmissions from the Cisco uBR7200 series CMTS.<br>Valid values are from 1 to 200 msec.<br>Default = 10 msec. |
| **no cable sync-interval** | Returns the sync message interval to its default value of 10 msec. |

## Verifying Sync Message Interval

To determine if a sync message interval is configured, enter the **show running-config** command and look for the cable interface configuration information. If the sync message interval is deactivated or reset to its default value, the `no sync interval` command line appears in the output.

# Configuring Basic Broadband Internet Access

This chapter describes the parameters of configuring and maintaining basic broadband Internet access. The chapter contains these sections:


- "Overview of Basic Broadband Internet Access" section on page 6-1
- "Recommended Basic Configuration for High-Speed Internet Access" section on page 6-2
- "Basic Internet Access Sample Configuration File" section on page 6-3


## Overview of Basic Broadband Internet Access

A Cisco uBR7200 series router and an intermediate frequency (IF)-to-radio frequency (RF) upconverter are installed at the headend or distribution hub to transmit digital data. The Cisco uBR7200 series router downstream ports transmit IF signals to the upconverter, which translates the downstream signals to RF for broadcast.

Receivers, scramblers, and descramblers then process the TV signals to encode or decode signals as needed for broadcast. Modulators format the analog TV and digital signals.

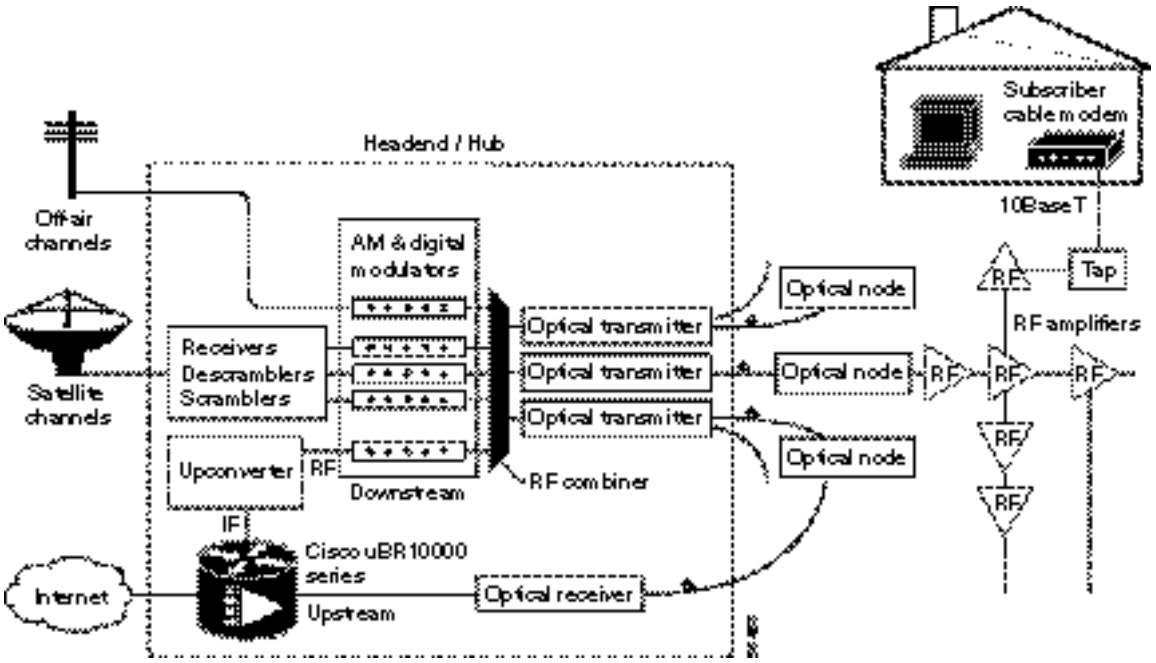
The analog and digital signals then pass through the RF combiner. The signals are broadcast from the headend through optical transmitters to fiber nodes.

Amplifiers, coaxial cable, and taps carry the signals to the subscriber premises. Signals are processed as follows:

- Tuners that handle MPEG video, audio, and broadcast services in set-top boxes (STBs), TVs, and VCRs receive one-way analog signals.
- CMs receive digital data signals:
  - Two-way CMs transmit RF signals back through amplifiers to optical fiber receivers at the headend. These receivers pass the upstream signal to upstream ports on the Cisco uBR7200 series router, where they are processed.

Figure 6-1 on page 6-2 illustrates this general signal flow and associated processes in the CMTS.

*Figure 6-1 Two-Way Internet Access Network Example*




Note The external upconverter shown in Figure 6-1 is needed only if you are not using the router's integrated upconverter.

# Recommended Basic Configuration for High-Speed Internet Access

The Cisco uBR7200 series router is fully capable of self-provisioning all CMs and hosts to which it is attached. The router supports multiple IP subnets, including different subnets for hosts and CMs. Configuration options are limited only by available configuration file length.

The Cisco uBR7200 series CMTS automatically connects DOCSIS-compliant CMs and hosts right out of the box. Therefore, the factory-supplied configuration activates the downstream RF to 851 MHz center frequency, and the upstream to 37 MHz.

Step 1 Connect one upstream port and the downstream port to a duplex filter.

Note Do not combine multiple ports, because they are all set on the same frequency.

Step 2 Use at least 40 dB attenuation before the first modem, and modems will connect in under 5 minutes.

# Basic Internet Access Sample Configuration File

## General

The following sample configuration file for the Cisco uBR7200 series router includes the following features:

- Basic DOCSIS Internet Access
- DHCP Address Pools—The Cisco uBR7200 series router acts as a DHCP server, providing different address spaces on the basis of the CM's service level, including those customers whose network access should be denied access because they have cancelled their service. Different default pools can be used for CMs and for the IP hosts behind them. Static IP addresses can also be assigned to specific clients on the basis of the client's MAC address.
- DOCSIS CM Configuration Files—These configuration files provide several different service level options:
  - platinum.cm—Users are given a maximum upstream bandwidth of 128 kbps, with a guaranteed minimum bandwidth of 10 kbps. The downstream has a maximum bandwidth of 10 Mbps. Up to 8 PCs are allowed on this connection.
  - gold.cm—Users are given a maximum upstream bandwidth of 64 kbps and a maximum downstream bandwidth of 5 Mbps. Up to 3 PCs are allowed on this connection.
  - silver.cm—Users are given a maximum upstream bandwidth of 64 kbps and a maximum downstream bandwidth of 1 Mbps. Only 1 PC is allowed on this connection.
  - disable.cm—Users are denied access to the cable network. This configuration file can be used for users who have cancelled service or have not paid their bills.

```
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service compress-config
service udp-small-servers max-servers 500
!
hostname uBR7200
!
boot system slot0:
!
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable time-server
!
cable config-file platinum.cm
   service-class 1 max-upstream 128
   service-class 1 guaranteed-upstream 10
   service-class 1 max-downstream 10000
   service-class 1 max-burst 1600
   cpe max 8
   timestamp
!
cable config-file gold.cm
   service-class 1 max-upstream 64
   service-class 1 max-downstream 5000
   service-class 1 max-burst 1600
   cpe max 3
   timestamp
!
```

```
cable config-file silver.cm
   service-class 1 max-upstream 64
   service-class 1 max-downstream 1000
   service-class 1 max-burst 1600
   cpe max 1
   timestamp
!
cable config-file disable.cm
   access-denied
   service-class 1 max-upstream 1
   service-class 1 max-downstream 1
   service-class 1 max-burst 1600
   cpe max 1
   timestamp
!
ip subnet-zero
ip cef
no ip domain-lookup
ip dhcp excluded-address 10.128.1.1 10.128.1.15
ip dhcp excluded-address 10.254.1.1 10.254.1.15
ip dhcp ping packets 1
!
ip dhcp pool CableModems
     network 10.128.1.0 255.255.255.0
     bootfile platinum.cm
     next-server 10.128.1.1
     default-router 10.128.1.1
     option 128 ip 10.128.1.1
     option 4 ip 10.128.1.1
     option 2 hex ffff.8f80
     option 11 ip 10.128.1.1
     option 10 ip 10.128.1.1
     lease 1 0 10
!
ip dhcp pool hosts
     network 10.254.1.0 255.255.255.0
     next-server 10.254.1.1
     default-router 10.254.1.1
     dns-server 10.254.1.1 10.128.1.1
     domain-name ExamplesDomainName.com
     lease 1 0 10
!
ip dhcp pool staticPC(012)
     host 10.254.1.12 255.255.255.0
     client-identifier 0108.0009.af34.e2
     client-name staticPC(012)
     lease infinite
!
ip dhcp pool goldmodem
     host 10.128.1.129 255.255.255.0
     client-identifier 0100.1095.817f.66
     bootfile gold.cm
!
ip dhcp pool DisabledModem(0010.aaaa.0001)
     host 10.128.1.9 255.255.255.0
     client-identifier 0100.1095.817f.66
     bootfile disable.cm
!
ip dhcp pool DisabledModem(0000.bbbb.0000)
     client-identifier 0100.00bb.bb00.00
     host 10.128.1.10 255.255.255.0
     bootfile disable.cm
!
interface Cable5/0
```

```
   description Cable Downstream Interface
   ip address 10.254.1.1 255.255.255.0 secondary
   ip address 10.128.1.1 255.255.255.0
   no keepalive
   cable downstream annex B
   cable downstream modulation 64qam
   cable downstream interleave-depth 32
   cable downstream frequency 851000000
   cable down rf-power 55
   cable upstream 0 description Cable upstream interface, North
   cable upstream 0 frequency 37008000
   cable upstream 0 power-level 0
   cable upstream 0 admission-control 150
   no cable upstream 0 shutdown
   cable upstream 1 description Cable upstream interface, South
   cable upstream 1 frequency 37008000
   cable upstream 1 power-level 0
   cable upstream 1 admission-control 150
   no cable upstream 1 shutdown
   cable upstream 2 description Cable upstream interface, East
   cable upstream 2 frequency 37008000
   cable upstream 2 power-level 0
   cable upstream 2 admission-control 150
   no cable upstream 2 shutdown
   cable upstream 3 description Cable upstream interface, West
   cable upstream 3 frequency 37008000
   cable upstream 3 power-level 0
   cable upstream 3 admission-control 150
   no cable upstream 3 shutdown
   no cable arp
   cable source-verify dhcp
   cable dhcp-giaddr policy
!
ip classless
no ip forward-protocol udp netbios-ns
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
ip http server
!
!
alias exec scm show cable modem
alias exec scf show cable flap
alias exec scp show cable qos profile
!
line con 0
   transport input none
line aux 0
line vty 0 4
   login
!
end
```

To set up spectrum management in your configuration, use the following commands to set up the critical elements:

```
cable spectrum-group 1 frequency 40000000
cable spectrum-group 1 frequency 20000000 2
```

In this illustration, the user has configured spectrum management group number “1” to be available to upstream channels. As defined by the two previous command lines, the “preferred” choice is for the upstream to operate on a 40-MHz channel. If that channel is not suitable for the transmission scheme available, the upstream automatically moves over to transmitting at 20 MHz and increases the receive power rating by 2 dB.

The command lines in the sample configuration file beginning with the **cable modulation-profile** command contain the critical elements necessary to set up a modulation profile in your overall configuration:

```
cable modulation-profile 3 request 0 16 1 8 16qam scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 3 initial 5 34 0 48 16qam scrambler 152 no-diff 256 fixed uw16
cable modulation-profile 3 station 5 34 0 48 16qam scrambler 152 no-diff 256 fixed uw16
cable modulation-profile 3 short 5 75 6 8 16qam scrambler 152 no-diff 144 fixed uw8
cable modulation-profile 3 long 8 220 0 8 16qam scrambler 152 no-diff 160 fixed uw8
```

In this case, the user has configured modulation profile number “3” to be available to upstream channels wherever they are configured to apply it. Note that this modulation profile has been configured to operate with a QAM-16 modulation scheme. The default modulation scheme for any upstream profile (if it is not set to QAM-16) is QPSK.

Later in the configuration file example, upstream port 0 on the cable interface card installed in slot 5 uses both the spectrum management and the modulation profile configured in the sample:

```
cable upstream 0 spectrum-group 1
cable upstream 0 modulation-profile 3
```

# Overview of the Cisco Network Registrar for the Cisco uBR7200 Series

This chapter supplements the Cisco Network Registrar (CNR) documentation by providing additional cable-specific instructions that are pertinent to the Cisco uBR7200 series and CMTS management.

For additional information about CNR, refer to these documents on Cisco.com:

- *Cisco Network Registrar for the Cisco uBR7200 Series Universal Broadband Routers*
- *CNR and DHCP FAQs for Cable Environment*
- *Recommended CNR Settings and Management*
- *Cable Technology Technical Tips*

## Cisco Network Registrar Description

CNR is a dynamic IP address management system, currently running on Windows NT or Solaris 2.6, that uses the Dynamic Host Configuration Protocol (DHCP) to assign IP addresses to cable interfaces, PCs, and other devices on the broadband network. The CNR tool includes script extensions that allow a cable system administrator to define and view individual DHCP options, define the identity or type of device on the network, and assign the device to a predefined class or group.

Using the CNR tool, a cable system administrator can specify policies to provide:

- Integrated DHCP and Domain Name Server (DNS) services
- Time of Day (ToD) and Trivial File Transfer Protocol (TFTP) server based on the size of the network
- DHCP safe failover and dynamic DNS updates

Note This is available only in CNR 3.0 or higher.

Using the CNR tool and the extension scripts identified in the "Overview of Scripts" section, a cable system administrator can specify scopes, policies, and options for the network and each cable interface based on the services and configuration to support at each subscriber site.

Note Scopes refer to the administrative grouping of TCP/IP addresses; all IP addresses within a scope should be on the same subnet.

The cable system administrator defines system default policies for all standard options and uses scope-specific policies for options related to particular subnets, such as cable interfaces. This allows DHCP to send the information with the IP address.

Seven entry points exist for scripts:

- post-packet-decode

- pre-client-lookup
- post-client-lookup—Examines and takes action on results of the client-class process, places data items in the environment dictionary to use at the pre-packet-encode extension point, includes DHCP relay option
- check-lease-acceptable
- pre-packet-encode
- post-sent-packet
- pre-dns-add-forward

## Cable Modem DHCP Response Fields

Each cable interface on the broadband network requires the following fields in the DHCP response:

- CM's IP address
- CM's subnet mask

Note For cable operators with less experience in networking, you can fill in a guess based on the network number and indicate how your IP network is divided.

- Name of the DOCSIS configuration file on the TFTP server intended for the cable interface
- Time offset of the cable interface from the Universal Coordinated Time (UTC), which the cable interface uses to calculate the local time when time-stamping error logs
- Time server address from which the cable interface obtains the current time

## DOCSIS DHCP Fields

DOCSIS DHCP option requirements include:

- IP address of the next server to use in the TFTP bootstrap process; this is returned in the siaddr field
- DOCSIS configuration file that the cable interface downloads from the TFTP server

Note If the DHCP server is on a different network that uses a relay agent, then the relay agent must set the gateway address field of the DHCP response.

- IP address of the security server should be set if security is required

## DHCP Relay Option (DOCSIS Option 82)

DOCSIS Option82 modifies DHCPDISCOVER packets to distinguish cable interfaces from the CPE devices or "clients" behind them. The DOCSIS Option82 is comprised of the following two suboptions:

- Suboption 1, Circuit ID:

```
Type 1 (1 byte)
Len 4 (1 byte)
Value (8 bytes)
<bit 31,30,.....................0)
<xYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY>
```

where the MSB indicates if the attached device is a cable interface.

`x=1 Cable Modem REQ`

`x=0 CPE device`
(Behind the cable interface with the cable interface MAC address shown in suboption 2.)

The rest of the bits make up the SNMP index to the CMTS interface.

`Y=0xYYYYYYY` is the SNMP index to the CMTS interface.

- Suboption 2, MAC address of the cable interface:

```
Type 2 (1 byte)
Len 6 (1 byte)
Value xxxx.xxxx.xxxx (6 bytes)
```

For additional information about

# Overview of Scripts

This section lists the scripts applicable to cable interface configuration.

## Two-way Cable Modem Scripts

To support two-way configurations at a subscriber site, use these scripts:

- **Relay.tcl**
- **SetRouter.tcl**

## Telco Return Cable Modem Scripts

To support telco return and two-way cable interface configurations on the same cable interface card or chassis, use these scripts:

- **PostClientLookup.tcl**
- **PrePacketEncode.tcl**

# Placement of Scripts

## Windows NT

For CNR running on Windows NT, place the appropriate scripts in the following directory:

```
\program files\network registrar\extensions\dhcp\scripts\tcl
```

## Solaris

For CNR running on Solaris, place the appropriate scripts in the following directory:

```
/opt/nwreg2/extensions/dhcp/scripts/tcl
```

# Activate Scripts in Cisco Network Registrar

To activate the scripts after you have placed them in the appropriate directory:

Step 1 Open up a text editor.

Step 2 Open one of the scripts at the **nrcmd>** command prompt.

Step 3 Create the extension points and attach them to the system.

Note The easiest way to do this is to simply cut and paste the command lines from the scripts to the **nrcmd>** command line.

Step 4 After you have created and attached the extension points, do a **dhcp** reload.

The scripts are active.

# Configuring the Cisco uBR7200 Series to Use Scripts

Each cable interface must be set up as a BOOTP forwarder and have the relay-option enabled. The primary and secondary IP addresses for each cable interface must be in sync with the CNR tool.

To properly communicate with scripts in the system, implement the following commands on the Cisco uBR7200 series universal broadband router:

- On Cisco IOS Release 11.3—Command is interface specific:

  ```
  cable relay-agent-option
  ```

  This enables Option82 on the Cisco uBR7200 series.

- On Cisco IOS Release 12.0—Command has been changed to the following global option:

  ```
  ip dhcp relay info option
  ```

- On Cisco IOS Release 12.0 to 12.5, use the following command:

  ```
  no ip dhcp relay information option check
  ```

Note You can also use the **cable dhcp-giaddr** command in cable interface configuration mode to modify the GIADDR field of DHCPDISCOVER and DHCPREQUEST packets to provide a relay IP address before packets are forwarded to the DHCP server. Use this command to set a “policy” option such that primary addresses are used for CMs and secondary addresses are used for hosts behind the CMs.

# Configure the System Default Policy

Add these options to the system default policy for:

- Cable modems to support on your network
- PCs to support behind each cable interface on your network

## Cable Modems

Define these settings following the CNR tool documentation:

- TFTP server (IP address) for those cable interfaces using BOOTP
- Time-server (IP address)
- Time-offset (Hex value, 1440 for Eastern Standard Time)
- Packet-siaddr (IP address of CNR)
- Router (set to 0.0.0.0)
- Boot-file (name of .cm file for those cable interfaces using BOOTP)
- Packet-file-name (.cm file name)

## PCs

Define these settings following the CNR tool documentation:

- Domain name
- Name servers (IP address of DNS servers)

# Create Selection Tag Scopes

## General

When you create your scope selection tags:

Step 1 Cut and paste the scope **selection tag create** commands from the scripts into the **nrcmd>** command line.

Note These names have to be exactly as they appear in the scripts.

Step 2 Then attach the selection tags to the appropriate scripts:

Example:

```
CM_Scope tagCablemodem
PC_Scope tagComputer
```

## Telco Return

Note If you are using the **prepacketencode** and **postclientlookup .tcl** scripts for telco return, the telco return scope does not have a selection tag associated to the scope.

Step 1 Put the tag **Telcocablemodem** on the primary cable interface scope to pull addresses from that pool instead.

Step 2 Follow the same procedure as above, but use a telco return policy which has a different .cm file with telco-specific commands in it.

# Create Network Scopes

Following is an example for creating scopes for your network. This example assumes two Cisco uBR7200 series universal broadband routers in two locations, with one cable interface card on one Cisco uBR7200 series configured for telco return.

```
cm-toledo1_2-0 10.2.0.0 255.255.0.0 assignable 10.2.0.10-10.2.254.254 tagCablemodem
tagTelcomodem Default GW=10.2.0.1 (assigned by scripts)

cm-toledo1_3-0 10.3.0.0 255.255.0.0 assignable 10.3.0.10-10.3.254.254 tagCablemodem
tagTelcomodem Default GW=10.3.0.1 (assigned by scripts)

pc-toledo1_2-0 208.16.182.0 255.255.255.248 assignable 208.16.182.2-208.16.182.6
tagComputer Default GW=208.16.182.1 (assigned by scripts)

pc-toledo1_3-0 208.16.182.8 255.255.255.248 assignable 208.16.182.10-208.16.182.14
tagComputer Default GW=208.16.182.9 (assigned by scripts)

telco_return_2-0 192.168.1.0 255.255.255.0 (No assignable addresses, tag was put on cable
modem primary scope to force telco-return cable modem to pull address from primary scope)

cm-arlington1_2-0 10.4.0.0 255.255.0.0 assignable 10.4.0.10-10.4.254.254 tagCablemodem
Default GW=10.4.0.1 (assigned by scripts)

cm-arlington1_3-0 10.5.0.0 255.255.0.0 assignable 10.5.0.10-10.5.254.254 tagCablemodem
Default GW=10.5.0.1 (assigned by scripts)

pc-arlington1_2-0 208.16.182.16 255.255.255.248 assignable 208.16.182.17-208.16.182.22
tagComputer Default GW=208.16.182.17 (assigned by scripts)

pc-toledo1_3-0 208.16.182.24 255.255.255.248 assignable 208.16.182.2-208.16.182.30
tagComputer Default GW=208.16.182.25 (assigned by scripts)
```

Note Remember the last valid address in the .248 subnet range is the broadcast address; do not use this.

# Create Policies for Class of Service or for Upgrading Cable Modem Cisco IOS Images

To support Class of Service (CoS), define:

- Scope selection tags—Identifiers that describe types of scope configurations

  Note This is needed for Option82.

- Client classes—Class with which a group of clients is associated

  Note Scope selection tags are excluded from or included in client-classes.

- Client—Specific DHCP clients and the defined class to which they belong

To assign the CoS or use Option82, make a client entry with a MAC address and point to the appropriate policy. To use client-based MAC provisioning, add a client entry "default - exclude," then put in MAC addresses for all devices (for example, cable interfaces and PCs) in the client tab and select the policy to use, including the appropriate tag.

Note For more detailed information about Cisco Network Registrar, please refer to the document *Cisco Network Registrar for the Cisco uBR10000 Series Universal Broadband Routers*.

# CNR Steps to Support Subinterfaces

The CNR configuration is done differently if subinterfaces are configured. Here is an example. If you have configured two ISP subinterfaces and one management subinterface on a Cisco uBR7200 series, make sure that the management subinterface is the first subinterface that is configured. If cable interface three—c3/0—is being used, create c3/0.1, c3/0.2 and c3/0.3 as three subinterfaces and c3/0.1 as the first subinterface configured as the management subinterface.

Note The Cisco uBR7200 series requires management subinterfaces to route DHCP packets from CMs when they first initialize because the Cisco uBR7200 series does not know the subinterfaces they belong to until it has seen the IP addresses assigned to them by gleaning DHCP reply message from CNR.

In CNR, complete the following steps for such a configuration:

Step 1 Create two scope selection tags such as: **isp1-cm-tag** and **isp2-cm-tag**

Step 2 Configure three scopes; for example, **mgmt-scope**, **isp1-cm-scope**, and **isp2-cm-scope** such that **isp1-cm-scope** and **isp2-cm-scope** each define **mgmt-scope** to be the primary scope

Step 3 Also configure two scopes for PCs for each of the ISPs; **isp1-pc-scope** and **isp2-pc-scope**. For scope **isp1-cm-scope**, configure **isp1-cm-tag** to be the scope selection tag. For scope **isp2-cm-scope**, configure **isp2-cm-tag** to be the scope selection tag

Step 4 Configure two client classes; for example, **isp1-client-class** and **isp2-client-class**

Step 5 Create client entries with their MAC addresses for CMs that belong to **ISP1** and assign them to **isp1-client-class.** Also assign the scope selection tag **isp1-cm-tag**

Step 6 Create client entries for CMs that belong to **ISP2** and assign them to **isp2-client-class**. Also assign the scope selection **tag isp2-cm-tag**

Step 7 Enable client class processing from the scope-selection-tag window

Note Overlapping address ranges cannot be configured on these subinterfaces because software gleans the DHCP reply to figure out the subinterface it really belongs to. Although CNR can be configured with overlapping address range scopes, it cannot be used to allocate addresses from these scopes.

# Troubleshooting the System

This chapter contains troubleshooting information for various functions of your Cisco uBR7200 series Cable Modem Termination System (CMTS) and includes the following sections:

| Section | Purpose |
|---|---|
| "Understanding show Command Responses" section on page 8-2 | Provides **show** command options for deriving system information. |
| "Using a Headend Cable Modem to Verify Downstream Signals" section on page 8-6 | Uses a Cisco uBR924 cable access modem to verify the downstream signal originating from a Cisco uBR7200 series router. |
| "Performing Amplitude Averaging" section on page 8-7 | The system uses an averaging algorithm to determine the optimum power level for a CM with low carrier-to-noise ratio that is making excessive power adjustments—known as flapping. This section shows how you can interpret these power adjustments as indicating unstable return path connections. |
| "Setting Downstream Test Signals" section on page 8-9 | Provides configuration commands that allow you to create downstream test signals. |
| "Pinging Unresponsive Cable Modems" section on page 8-10 | Allows a cable system administrator to quickly diagnose the health of a channel between the Cisco uBR7200 series cable interface and the CM. |
| "Using Cable Interface debug Commands" section on page 8-11 | Provides instructions for troubleshooting cable interface line cards. |

Note For detailed information about troubleshooting your CMTS platform using cable flap lists, refer to the chapter "Flap List Troubleshooting for the Cisco CMTS" in the *Cisco Cable Modem Termination System Feature Guide* on Cisco.com.

# Understanding show Command Responses

This section summarizes cable-related **show** commands. For additional command information about these and other CMTS commands, refer to these additional resources on Cisco.com:

- *Cisco Broadband Cable Command Reference Guide*
- *Cisco Cable Modem Termination System Feature Guide*

| Command | Purpose |
|---|---|
| show cable flap-list [*sort-interface* \| *sort-flap* \| *sort-time*] | To display the cable flap-list on a Cisco uBR7200 series router, use the **show cable flap-list** command in privileged EXEC mode.<br><br>For the Cisco uBR7200 series, the **sort** option applies to one line card at a time, then the list is merged together. For example, the flap list is sorted for cable7/0, appears on the console, and then is sorted for cable 7/1, which then appears on the console, and so on.<br><br>The **show cable flap-list** and **show cable modem** commands indicate when the Cisco uBR7200 series CMTS has detected an unstable return path for a particular modem and has compensated with a power adjustment. An asterisk (*) appears in the power-adjustment field for a modem when a power adjustment has been made; an exclamation point appears when the modem has reached its maximum power transmit level and cannot increase its power level any further.<br><br>For additional information about using cable flap lists, refer to the chapter "Flap List Troubleshooting for the Cisco CMTS" in the *Cisco Cable Modem Termination System Feature Guide*. |

| Command | Purpose |
|---|---|
| show cable modem | To display all Data-over-Cable Service Interface Specification (DOCSIS) states, and other useful troubleshooting information, such as last received upstream radio frequency (RF) power level and maximum number of provisioned customer premises equipment (CPE), use the **show cable modem** command in privileged EXEC mode.<br><br>Note DOCSIS CMs are required to pass through successive states during registration and provisioning. Using this information, you can isolate why a CM is offline or unavailable.<br><br>The **show cable flap-list** and **show cable modem** commands indicate when the Cisco uBR7200 series CMTS has detected an unstable return path for a particular modem and has compensated with a power adjustment. An asterisk (*) appears in the power-adjustment field for a modem when a power adjustment has been made; an exclamation point appears when the modem has reached its maximum power transmit level and cannot increase its power level any further.<br><br>The **show cable modem** command displays a list of options for a single modem to be specified by entering either the RF CPE device IP address or MAC address:<br><br>• Signal-to-noise ratio (SNR) information for each CM on each interface<br>• Summary display of the total number of modems connected for each upstream channel<br>• Total number of registered and unregistered modems for the specified interface or upstream<br>• Total number of offline modems for the specified interface or upstream, and status for each offline modem before it went offline |
| show cable modem maintenance | To display station maintenance error statistics, use the **show cable modem maintenance** command in privileged EXEC mode.<br><br>When a CM is detected to be offline by the CMTS—no reply after 16 retries of station maintenance requests—the CM is marked offline. Besides marking the CM and service identifier (SID) state offline, the SID is removed immediately from the CMTS ranging list, and an aging timer is started to clean up the SID completely if the CM does not attempt to come online within the next 24 hours.<br><br>Output fields are described below:<br><br>• The *SM Exhausted Count* value refers to the number of times a CM was dropped because it did not reply to station maintenance requests. A CM is removed from the station maintenance list after 16 times of periodic ranging opportunity without seeing the RNG_REQ from the modem.<br>• The *SM Aborted Count* value refers to the number of times the CM was dropped because its operational parameters were unacceptable. This includes such reasons as the power level is outside the acceptable range, or the timing offset keeps changing. The respective times in the command output indicate when this happened. |

| Command | Purpose |
|---|---|
| show cable qos profile | To display type of service (ToS) specifications, use the **show cable qos profile** command in privileged EXEC mode. Information includes upstream packet discards, errors, error-free packets, correctable and uncorrectable errors, noise, and micro-reflection statistics.<br><br>Following is a response to the **show cable qos profile** command. The display shows ToS specifications:<br><br>`Router# show cable qos profile`<br><br>`Service Prio Max Guarantee Max Max tx TOS TOS Create B`<br>`class upstream upstream downstream burst mask value by priv`<br>`> bandwidth bandwidth bandwidth enab`<br>`1 0 0 0 0 0 0x0 0x0 cmts(r) no`<br>`2 0 64000 0 1000000 0 0x0 0x0 cmts(r) no`<br>`3 0 1000 0 1000 0 0x0 0x0 cmts no`<br>`4 3 256000 0 512000 0 0x0 0x0 cm no`<br>`5 5 1000000 0 10000000 0 0x0 0x0 cm no`<br>`6 3 256000 0 512000 0 0x0 0x0 cm yes`<br><br>Note The "r" in the "Create by" column means that the first two classes of service the CMTS creates are reserved for CMs that are not online.<br><br>The optional argument *n* can be used to display a specific profile. |

| Command | Purpose |
|---|---|
| show interface cable | To display cable interface information, use the **show interface cable** command in privileged EXEC mode:<br><br>**show interface cable** *slot/port* [*downstream* \| *upstream*]<br><br>The following example displays **show interface cable** command output for a CM located in slot 1/port 0:<br><br>`Router# show interface cable 5/0`<br><br>`Cable5/0 is up, line protocol is up`<br>`  Hardware is BCM3210 FPGA, address is 00e0.1e5f.7a60 (bia 00e0.1e5f.7a60)`<br>`  Internet address is 1.1.1.3/24`<br>`  MTU 1500 bytes, BW 27000 Kbit, DLY 1000 usec, rely 255/255, load 1/255`<br>`  Encapsulation, loopback not set, keepalive not set`<br>`  ARP type: ARPA, ARP Timeout 04:00:00`<br>`  Last input 4d07h, output 00:00:00, output hang never`<br>`  Last clearing of “show interface” counters never`<br>`  Queuing strategy: fifo`<br>`  Output queue 0/40, 0 drops; input queue 0/75, 0 drops`<br>`  5 minute input rate 0 bits/sec, 0 packets/sec`<br>`  5 minute output rate 0 bits/sec, 0 packets/sec`<br>`  10908 packets input, 855000 bytes, 0 no buffer`<br>`  Received 3699 broadcasts, 0 runts, 0 giants, 0 throttles`<br>`  3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort`<br>`  5412 packets output, 646488 bytes, 0 underruns`<br>`  0 output errors, 0 collisions, 13082 interface resets`<br>`  0 output buffer failures, 0 output buffers swapped out`<br><br>The **show interface cable upstream** command is enhanced to display details on the MAC scheduler state for an upstream port.<br><br>New items in the display include:<br><br>• Detailed slot queue statistics—Queue [CIR Grants] 0/20, fair queuing, 0 drops in the previous example, meaning that the queue for CIR-service grants has a current depth of 0, and a maximum depth of 20. Weighted fair queuing shows grants in this queue.<br>• Constant bit rate (CBR) slot scheduling table state—The reserved slot table in the previous example has two CBR entries. This shows that at the time the command was issued, the MAC scheduler had admitted two CBR slots in the reserved slot table.<br>• Counters for each type of upstream slot scheduled in the MAPs for this upstream channel—The “Init Mtn IEs 800” means that the MAC scheduler has added 800 initial maintenance information elements (slots) at the time the **show** command was issued.<br>• MAC scheduling statistics—Displays the percentage of the upstream bandwidth that is used for each type of slot on an average. |

| Command | Purpose |
|---|---|
| show interface cable sid | To display the service identifier (SID) for a CM, use the **show interface cable sid** command in privileged EXEC mode.<br><br>The following sample output from the **show interface cable sid** command shows the one form of the command:<br><br>`Router# show int c4/0 sid`<br><br>`Sid Prim MAC Address IP Address Type Age Admin Sched Sfid State Type`<br>`5 0010.7b6b.58c1 10.20.114.34 stat 2d1h36menable BE 1`<br>`6 0010.7bed.9dc9 10.20.114.37 stat 2d1h36menable BE 13`<br>`7 0010.7bed.9dbb 10.20.114.38 stat 2d1h36menable BE 15`<br>`8 0010.7b6b.58bb 10.20.114.112 stat 2d1h34menable BE 17`<br>`9 0010.7b6b.58bb 10.20.114.112 dyna 2d1h34menable BE 19` |
| show cable modulation-profile | To display modulation profile group information for a Cisco CMTS, use the **show cable modulation-profile** command in privileged EXEC mode.<br><br>The **show cable modulation-profile** command now includes an added option number that displays the modulation profile number.<br><br>The **show cable modulation-profile** command completely replaces the former **show cable burst-profile** command. |

# Using a Headend Cable Modem to Verify Downstream Signals

You can use a Cisco uBR924 cable access modem to verify the downstream signal originating from a Cisco uBR7200 series router. Be sure that you configure the Cisco uBR924 according to DOCSIS CM practices.

To verify the downstream signal from a Cisco uBR7200 series router using a Cisco uBR924, follow the procedure below:

Step 1 After the Cisco uBR924 is operational and you have an input signal between 0 and +5 dBmV, use the **show controller c0 tuner** command.

Step 2 Scan the output for the value corresponding to the signal-to-noise (SNR) estimate variable. If this value is at least 35 dB, you have an optimized signal. If the value is less than 34 dB, adjust the upconverter at the cable headend.

Tip The SNR estimate for a CM installed at a headend should be between 35 and 39 dB. Although the exact value displayed varies from CM to CM, values collected on the same CM from measurement to measurement will be consistent. Maximizing SNR optimizes CM reliability and service quality.

# Performing Amplitude Averaging

The Cisco uBR7200 series CMTS uses an averaging algorithm to determine the optimum power level for a CM with low carrier-to-noise ratio that is making excessive power adjustments—known as flapping. To avoid dropping flapping CMs, the Cisco uBR7200 series CMTS averages a configurable number of RNG-REQ messages before it makes power adjustments. By compensating for a potentially unstable return path, the Cisco uBR7200 series CMTS maintains connectivity with affected CMs. You can interpret these power adjustments, however, as indicating unstable return path connections.

The **show cable flap-list** and **show cable modem** commands are expanded to indicate the paths on which the Cisco uBR7200 series CMTS is making power adjustments and the modems that have reached maximum transmit power settings. These conditions indicate unstable paths that should be serviced.

The following example shows the output of the **show cable flap-list** command:

```
Router# show cable flap-list
MAC Address     Upstream     Ins   Hit   Miss  CRC   P-Adj Flap  Time
 0010.7bb3.fd19  Cable5/0/U1  0     2792  281   0     *45    58    Jul 27 16:54:50
 0010.7bb3.fcfc  Cable5/0/U1  0     19    4     0     !43    43    Jul 27 16:55:01
 0010.7bb3.fcdd  Cable5/0/U1  0     19    4     0     *3     3     Jul 27 16:55:01
```

The asterisk (*) indicates that the CMTS is using the power-adjustment method on this modem. An exclamation point (!) indicates that the modem has reached maximum transmit power.

Output of the **show cable modem** command appears below:

```
Router# show cable modem
MAC Address    IP Address      I/F       MAC         Prim RxPwr Timing Num  BPI
                                         State       Sid  (db)  Offset CPEs Enbld
0050.04f9.edf6 10.44.51.49     C7/1/U0 online      1   -0.50  3757   0    no
0050.04f9.efa0 10.44.51.48     C7/1/U0 online      2   -0.50  3757   0    no
0030.d002.41f5 10.44.51.147    C7/1/U0 online      3   -0.25  3829   0    no
0030.d002.4177 10.44.51.106    C7/1/U0 online      4   -0.50  3798   0    no
0030.d002.3f03 10.44.51.145    C7/1/U0 online      5   0.25   3827   0    no
0050.04f9.ee24 10.44.51.45     C7/1/U0 online      6   -1.00  3757   0    no
0030.d002.3efd 10.44.51.143    C7/1/U0 online      7   -0.25  3827   0    no
0030.d002.41f7 10.44.51.140    C7/1/U0 online      8   0.00   3814   0    no
0050.04f9.eb82 10.44.51.53     C7/1/U0 online      9   -0.50  3756   0    no
0050.f112.3327 10.44.51.154    C7/1/U0 online      10  0.25   3792   0    no
0030.d002.3f8f 10.44.51.141    C7/1/U0 online      11  0.00   3806   0    no
0001.64f9.1fb9 10.44.51.55     C7/1/U0 online      12  0.00   4483   0    no
0030.d002.417b 10.44.51.146    C7/1/U0 online      13  0.50   3812   0    no
0090.9600.6f7d 10.44.51.73     C7/1/U0 online      14  0.00   4071   0    no
0010.9501.ccbb 10.44.51.123    C7/1/U0 online      15  0.25   3691   0    no
```

The asterisk (*) in the **show cable modem** command output indicates that the CMTS is using the power adjustment method on this CM. The ! symbol indicates that the CM has reached maximum transmit power.

This section documents the commands pertaining to amplitude averaging:

- **cable upstream power-adjust noise**
- **cable upstream frequency-adjust averaging**

## Enabling or Disabling Power Adjustment

To enable the power-adjustment capability, use the **cable upstream power-adjust** command in interface configuration mode:

**cable upstream** *n* **power-adjust** {**threshold** [*threshold #*] | **continue** [*tolerable value*] | **noise** [*% of power adjustment*]}

To disable the power-adjustment capability, use the **no** form of this command:

**no cable upstream power-adjust**

Syntax Description

| Syntax | Description |
|---|---|
| *n* | Specifies the upstream port number. |
| *threshold #* | Specifies the power-adjustment threshold. The threshold range is from 0 to 10 dB. The default is 1 dB. |
| *tolerable value* | Determines if the status of the RNG-RSP should be set to CONTINUE or SUCCESS. The range is from 2 to 15 dB. The default is 2 dB. |
| *% of power adjustment* | Specifies the percentage of power-adjustment packets required to switch from the regular power-adjustment method to the noise power-adjustment method. Range is from 10 to 100 percent. The default is 30 percent. |

Note The threshold default is 1 dB. The tolerable value default is 2 dB. The power adjustment is 30 percent.

Caution Default settings are adequate for system operation. Amplitude averaging is an automatic procedure. In general, Cisco does not recommend that you adjust values. Cisco does recommend, however, that you clean up your cable plant should you encounter flapping CMs.

Note In some instances, you might adjust certain values:

If CMs cannot complete ranging because they have reached maximum power levels, you might try to set the *tolerable value* CONTINUE field to a larger value than the default of 2 dB. Values larger than 10 dB on "C" versions of cable interface line cards, or 5 dB on FPGA versions, are not recommended.

If the flap list shows CMs with a large number of power adjustments, but the CMs are not detected as noisy, you might try to decrease the percentage for noisy. If you think that too many CMs are unnecessarily detected as noisy, you might try to increase the percentage.

## Setting Frequency Threshold to Affect Power Adjustment

To control power adjustment methods by setting the frequency threshold, use the **cable upstream freq-adj averaging in** interface configuration mode. To disable power adjustments, use the **no** form of this command.

**cable upstream** *n* **freq-adj averaging** *% of frequency adjustment*

**no cable upstream freq-adj averaging**

Syntax Description

| Syntax | Description |
|---|---|
| *n* | Specifies the upstream port number. |
| *averaging* | Specifies that a percentage of frequency adjustment packets is required to change the adjustment method from the regular power adjustment method to the noise power-adjustment method. |
| *% of frequency adjustment* | Specifies the percentage of frequency-adjustment packets required to switch from the regular power-adjustment method to the noise power-adjustment method. Valid range is from 10 to 100 percent. |

The following example shows how to change the power-adjustment method when the frequency adjustment packet count reaches 50 percent:

```
Router(config-if)# cable upstream 0 freq-adj averaging 50
```

# Setting Downstream Test Signals

This feature provides configuration commands that allow you to create downstream test signals. Both pseudo random bit stream (PRBS) and unmodulated carrier test signals are now supported.

A PRBS test signal is a random data pattern that has been modulated to look like a real data stream. An unmodulated test signal is a continuous sine wave that looks like a carrier wave on the downstream transmission.

See the following sections for the required tasks to create PRBS and unmodulated carrier test signals:


- "Configuring Unmodulated Test Signals" section on page 8-9
- "Configuring PRBS Test Signals" section on page 8-10
- "Verifying Test Signal Output" section on page 8-10


## Configuring Unmodulated Test Signals

| | Command | Purpose |
|---|---|---|
| Step 1 | `Router(config-if)# cable downstream if-output continuous-wave` | Generates an unmodulated continuous wave signal on the downstream channel. The interface is shut down. |
| Step 2 | `Router(config-if)# no cable downstream if-output` | Stops sending test signals.<br>Note Remember to reenable the interface to resume normal operations. |

## Configuring PRBS Test Signals

| | Command | Purpose |
|---|---|---|
| Step 1 | `Router(config-if)# cable downstream if-output prbs` | Generates a PRBS test signal on the downstream channel. The interface is shut down. |
| Step 2 | `Router(config-if)# no cable downstream if-output` | Stops sending test signals.<br>Note Remember to reenable the interface to resume normal operations. |

## Verifying Test Signal Output

To verify the output of a continuous wave test signal or the output of a PRBS test signal, use a spectrum analyzer on the downstream channel. The downstream carrier is enabled as a default.

The standard mode of operation is modulated signal output and the interface is active. For PRBS and continuous wave output, the selected interface is shut down.

The functioning of the **no cable downstream if-output** command has not changed. The interface is shut down.

# Pinging Unresponsive Cable Modems

## Pinging a Cable Modem

Ping DOCSIS is a Cisco patent-pending feature that allows a cable system administrator to quickly diagnose the health of a channel between the Cisco uBR7200 series routers and the cable interface. The technology uses 1/64—the bandwidth of IP ping—and works with CMs that do not have an IP address. This allows cable operators to ping CMs that are unable to complete registration, that have internal bugs, or that are unresponsive due to a crash.

The Ping DOCSIS feature includes a real-time view and plot of requested power adjustments, and a measure of optimal headend reception power. This gives the cable operator the ability to solicit a configurable number of periodic ranging requests from a cable interface.

To ping a specific cable interface to determine if it is online, use the following command in EXEC mode.

| | Command | Purpose |
|---|---|---|
| Step 1 | `Router# ping docsis addr` | Pings the CM with a specific MAC address or IP address to see if it is online. |

## Verifying the Ping

The **ping docsis** command returns a verification from a CM that is pinged:

```
Queuing 5 MAC-layer station maintenance intervals, timeout is 25 msec:
!!!!!
Success rate is 100 percent (5/5)
```

Tip If you are having trouble, make sure that you are using a valid MAC or IP address for the cable interface you want to ping.

# Using Cable Interface debug Commands

To troubleshoot cable interfaces, use the following **debug** commands in enable (privileged EXEC) mode.

| | Command | Purpose |
|---|---|---|
| Step 1 | **debug cable ?** | Displays all debug cable commands that are available. |
| Step 2 | **undebug all** | Turns off all debugging information to the console and chooses a more selective **debug** command.<br>Note Refer to the **debug** commands that follow. |

Caution The following commands can generate large amounts of output as the number of cable modems grows. On heavily loaded systems with thousands of CMs, these commands can dramatically affect router performance.

## debug cable arp

To activate the debugging of Address Resolution Protocol (ARP) requests on the cable interfaces, use the **debug cable arp** command in privileged EXEC mode. To deactivate debugging of ARP requests, use the **no** form of this command.

**debug cable arp**

When this command is activated, all cable ARP request messages are displayed on the Cisco uBR10000 series router console.

## debug cable error (for MAC Protocol Errors)

To display errors that occur in the cable MAC protocols, use the **debug cable error** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug cable error**

**no debug cable error**

When this command is activated, all cable ARP request messages are displayed on the Cisco uBR10000 series router console. When this command is activated, any errors that occur in the cable MAC protocol are displayed on the Cisco uBR10000 series router console.

# debug cable keyman (for Baseline Privacy Activity)

To activate the debugging of key encryption key (KEK) and traffic encryption key (TEK) BPI key management, use the **debug cable keyman** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug cable keyman**

**no debug cable keyman**

When this command is activated, all activity related to KEK and TEK keys appears on the Cisco uBR10000 series router console.

# debug cable mac-messages

To activate the debugging of messages generated in the cable MAC that frames and encrypts downstream RF signals, use the **debug cable mac-messages** command in privileged EXEC mode. To deactivate the debugging of cable MAC messages, use the **no** form of this command.

**debug cable mac-messages**

**no debug cable mac-messages**

When this command is activated, messages generated by the cable MAC are displayed on the Cisco Cisco uBR7200 series console.

# debug cable map

To display map debugging messages, use the **debug cable map** command in privileged EXEC mode. Use the **no** form of this command to disable debugging output.

**debug cable map sid [sid-num]**

**no debug cable map**

# debug cable phy

To activate the debugging of messages generated in the cable PHY, use the **debug cable phy** command in privileged EXEC mode. To deactivate the debugging of the cable PHY, use the **no** form of this command.

**debug cable phy**

**no debug cable phy**

Cable PHY is the physical layer where upstream and downstream activity between the Cisco uBR10000 series router and the HFC network is controlled. When this command is activated, messages generated in the cable PHY are displayed on the Cisco uBR10000 series router console.

# debug cable privacy (for Baseline Privacy)

To activate the debugging of baseline privacy, use the **debug cable privacy** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug cable privacy**

**no debug cable privacy**

# debug cable qos

To activate the debugging of QoS, use the **debug cable qos** command in privileged EXEC mode. To deactivate debugging of QoS, use the **no** form of this command.

**debug cable qos**

**no debug cable qos**

When this command is activated, messages related to QoS parameters are displayed on the Cisco uBR10000 series router console.

# debug cable range (for Ranging Messages)

To activate the debugging of ranging messages from cable interfaces on the HFC network, use the **debug cable range** command in privileged EXEC mode. To deactivate debugging of cable interface ranging, use the **no** form of this command.

**debug cable range**

**no debug cable range**

When this command is activated, ranging messages generated when cable interfaces request or change their upstream frequencies are displayed on the Cisco uBR10000 series router console.

# debug cable receive (for Upstream Messages)

To activate the debugging of upstream messages from cable interfaces, use the **debug cable receive** command in privileged EXEC mode. To deactivate debugging of upstream messages, use the **no** form of this command.

**debug cable receive**

**no debug cable receive**

When this command is activated, any messages generated by cable interfaces and sent to the Cisco uBR7200 series router are displayed on the router console.

## debug cable reg (for Modem Registration Requests)

To activate the debugging of registration requests from cable interfaces on the HFC network, use the **debug cable reg** command in privileged EXEC mode. To deactivate debugging of cable registration, use the **no** form of this command.

**debug cable reg**

**no debug cable reg**

When this command is activated, messages generated by cable interfaces as they make requests to connect to the network are displayed on the Cisco uBR10000 series router console.

## debug cable reset (for Reset Messages)

To activate the debugging of reset messages from cable interfaces on the HFC network, use the **debug cable reset** command in privileged EXEC mode. To deactivate debugging of cable reset messages, use the **no** form of this command.

**debug cable reset**

**no debug cable reset**

When this command is activated, reset messages generated by cable interfaces are displayed on the Cisco uBR10000 series router console.

## debug cable specmgmt (for Spectrum Management)

To activate the debugging of spectrum management (frequency agility) on the HFC network, use the **debug cable specmgmt** command in privileged EXEC mode. To deactivate debugging of cable spectrum management, use the **no** form of this command.

**debug cable specmgmt**

**no debug cable specmgmt**

When this command is activated, messages generated because of spectrum group activity are displayed on the Cisco uBR10000 series router console. Spectrum group activity can be additions or changes to spectrum groups, or frequency and power level changes controlled by spectrum groups.

## debug cable startalloc (for Channel Allocations)

To activate the debugging of channel allocations on the HFC network, use the **debug cable startalloc** command in privileged EXEC mode. To deactivate debugging of cable channel allocations, use the **no** form of this command.

**debug cable startalloc**

**no debug cable startalloc**

When this command is activated, messages generated when channels are allocated to cable interfaces on the HFC network are displayed on the Cisco uBR10000 series router console.

## debug cable transmit (for CMTS Transmissions)

To activate the debugging of transmissions from the Cisco uBR10000 series router across the HFC network, use the **debug cable transmit** command in privileged EXEC mode. To deactivate debugging of cable transmissions, use the **no** form of this command.

**debug cable transmit**

**no debug cable transmit**

```
When this command is activated, messages generated at the headend are displayed on the
Cisco uBR10000 series router console.
```

## debug cable ucc (for Upstream Channel Change Messages)

To activate the debugging of upstream channel change (UCC) messages generated when cable interfaces request or are assigned a new channel, use the **debug cable ucc** command in privileged EXEC mode. To deactivate debugging of cable upstream channel changes, use the **no** form of this command.

**debug cable ucc**

**no debug cable ucc**

When this command is activated, messages related to upstream channel changes are displayed on the Cisco uBR10000 series router console.

## debug cable ucd (for Upstream Channel Description Messages)

To activate the debugging of upstream channel descriptor (UCD) messages, use the **debug cable ucd** command in privileged EXEC mode. To deactivate debugging of cable upstream channel descriptor, use the **no** form of this command:

**debug cable ucd**

**no debug cable ucd**

UCD messages contain information about upstream channel characteristics and are sent to the cable modems on the HFC network. CMs that are configured to use enhanced upstream channels use these UCD messages to identify and select an enhanced upstream channel to use. When this command is activated, messages related to upstream channel descriptors are displayed on the Cisco uBR10000 series router console.

# Installing or Upgrading Cisco IOS Software

## Introduction

This appendix explains how to install Cisco IOS software onto "run-from-RAM" Cisco routers using a TFTP server or remote copy protocol (rcp) server application.

The information in this document describes Cisco IOS Release 11.2 or later.

## Before You Begin

Perform these steps prior to installing or upgrading Cisco IOS software:

Step 1 Install a TFTP server.

A TFTP server or a RCP server application must be installed on a TCP/IP-ready workstation or PC. After the application is installed, a minimal level of configuration must be performed.

a. Configure the TFTP application to operate as a TFTP server, as opposed to a TFTP client.

b. Specify the outbound file directory. This is the directory in which the Cisco IOS software images are stored (see Step 2 below). Most TFTP applications provide a setup routine to assist in these configuration tasks.

Note The TFTP server included on the software feature pack CD-ROM can be used on a PC running Windows 95. For other operating system s, a number of TFTP or rcp applications are available from independent software vendors or as shareware from public sources on the World Wide Web. The TFTP Server application included on the software feature pack CDs is also available on Cisco.com.

c. Download a TFTP server for Windows 95.

Step 2 Download the Cisco IOS software image onto your workstation or PC.

- You also need to have a valid Cisco IOS software image for your router. Make sure that the image supports your hardware and software features, and that your router has enough memory to run the image. If you do not yet have a Cisco IOS software image, or if you are not sure that the image you have meets all the necessary requirements, see *How to Choose a Cisco IOS Software Release* on Cisco.com.

You should now have a TFTP server installed, with a valid Cisco IOS software image.

# Installing or Upgrading Cisco IOS Software

Note For remote copy program (rcp) applications, substitute rcp for every occurrence of TFTP. For example, use the **copy rcp flash** command instead of the **copy tftp flash** command.

Step 1 Establish a console session to the router. Do this with either a direct console connection or a virtual Telnet connection. A direct console connection is preferred over a Telnet connection, because a Telnet connection gets lost during the reboot phase of the software installation. The console connection is made with a rolled cable (usually a flat black cable), and connects the console port of the router to the COM port of the PC. Open Hyperterminal on the PC, and use the following settings:

```
Speed 9600 bits per second
8 databits
0 parity bits
1 stop bit
No Flow Control
```

Step 2 Verify that the TFTP server has IP connectivity to the router.

Check the IP addresses of the TFTP server and the router (access server) targeted for the TFTP software upgrade to be sure that the addresses are within the same range. Ping the router (access server) to verify that a network connection exists between them. More information on IP addresses is available in Appendix B, “Resolving Common Image Installation Problems.”

Step 3 Copy the new software image from the TFTP server to the router (access server) using the following commands:

```
Router> enable
Password: password
Router#
Router# copy tftp flash
```

Note When you are connected to the router through the console port, if you get a > or `rommon >` prompt, your router is in ROM monitor (ROMMON) mode. If necessary, consult the *Boot Failure Recovery Procedures* on Cisco.com.

If necessary, you can copy an image from one device to another.

Note Cisco recommends that you keep a copy of the router or access server configuration before upgrading the router or access server software. The upgrade itself does not affect the configuration, which is stored in nonvolatile RAM (NVRAM).

Step 4 When prompted, enter the IP address of the TFTP server as in the following example:

```
Address or name of remote host [255.255.255.255]? 172.17.247.195
```

Step 5 When prompted, enter the filename of the Cisco IOS software image to be installed, as in the following example:

```
Source file name? ubr7200-k8p-mz
```

Note The image name varies depending on the filename of the image on the TFTP server.

Step 6 Specify the destination filename:

```
Destination file name? ubr7200-k8p-mz
```

This is the name the new software image will have when it is loaded onto the router. The image can be named anything, but common practice is to enter the UNIX image filename.

Step 7 Erase the Flash device before confirming:

a. Enter **yes** to erase the existing software image resident in the router's Flash memory before copying the new one.

b. Enter **no** to keep the existing software image. Be sure that you have enough Flash memory to keep both.

```
Erase flash device before writing? [confirm] yes/no
```

The copying process requires several minutes; the time differs from network to network. During the copying process, messages are displayed to indicate which files have been accessed.

The exclamation point "!" indicates that the copying process is taking place. Each exclamation point indicates that ten packets have been transferred successfully. A checksum verification of the image occurs after the image is written to Flash memory.

Step 8 Before reloading, verify the correct installation and commands.

a. Verify that the image is properly installed and that the boot system commands point to the proper file to load. Information about verifying the image and boot commands is available in Appendix B, “Resolving Common Image Installation Problems.”

b. To reload the image, type:

```
Router# reload
*Mar 1 00:30:49.972: %SYS-5-CONFIG_I: Configured from console by console
System configuration has been modified. Save? [yes/no]: no !-- lower case
Proceed with reload? [confirm] yes !-- lower case
```

Step 9 Use the **show version** command to verify that the router is running with the proper image.

# Sample Output—Cisco uBR7200 Series Router

```
Router# show flash

-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. unknown  317FBA1B  4A0694   24  4720148 Aug 29 1997 17:49:36
hampton/nitro/c7200-j-mz
2   .. unknown  9237F3FF  92C574   11  4767328 Oct 01 1997 18:42:53 c7200-js-mz
3   .D unknown  71AB01F1 10C94E0   10  7982828 Oct 01 1997 18:48:14 rsp-jsv-mz
4   .D unknown  96DACD45 10C97E0    8      639 Oct 02 1997 12:09:17 the_time
5   .. unknown  96DACD45 10C9AE0    3      639 Oct 02 1997 12:09:32 the_time
6   .D unknown  96DACD45 10C9DE0    8      639 Oct 02 1997 12:37:01 the_time
7   .. unknown  96DACD45 10CA0E0    8      639 Oct 02 1997 12:37:13 the_time

3104544 bytes available (17473760 bytes used)
```

# Related Information

The following documents on Cisco.com contain additional information related to software installation and upgrade:

- *How to Choose a Cisco IOS Software Release*
- *Field Notice: Cisco IOS TFTP Client Cannot Transfer Files Larger than 16MB in Size*

# Copying a System Image from One Device to Another

## Copying from Device to Device Inside the Same Router

The table below provides command options for copying a system image from one device to another. Methods vary according to different platforms.

The three most common commands used for image copying are:

**copy tftp flash**

**copy rcp flash**

**copy slot0: slot1:**

Refer to the *Cisco IOS Configuration Fundamentals Command Reference,* Release 12.1 on Cisco.com.

### Detailed Example

```
Router# show slot0
     -#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------  name
     1 .D unknown 5E8B84E6 209D8 11 2392 Jan 22 2000 00:22:42 flashconfig
     2 ..  image 5E7BAE19 B623C4 22 11802988 Jan 22 2000 00:23:18 rsp-jsv-mz.1 20-8.0.2.T

Router# show slot1:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------  name
1 .. unknown 6A2B4BA7 6FA9E0 20 7186784 Jul 30 1999 15:05:19 rsp-jv-mz.11  1-26.CC1
2 .. config 631F0D8B 6FB1EC 6 1929 Oct 19 1999 06:15:49 config
3 .. config  631F0D8B 6FB9F8 7 1929 Oct 19 1999 06:16:03 config1

Router# copy slot0: slot1
Source  filename []? rsp-jsv-mz.120-8.0.2.T
Destination filename [slot1]?
CCCCCCCCCCCCCCCCCCC
2392 bytes copied in 0.300 secs
```

## Copying from One Router to Another

Perform these steps in global configuration mode.

Step 1 Display the system Flash directory with the **show flash** command:

```
Router# show flash

System flash directory:
File  Length   Name/status
1   11173264  c2500-jos56i-l.120-9.bin
[11173328 bytes used, 5603888 available, 16777216 total]
16384K bytes of processor board System flash (Read ONLY)
```

Step 2 Activate the TFTP server on the router that has the Cisco IOS software image that you want to copy. The example below provides the command sequence to use:

```
Router# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# tf
Router(config)# tftp-server ?
flash:   Allow URL file TFTP load requests
flh:     Allow URL file TFTP load requests
lex:     Allow URL file TFTP load requests
null:    Allow URL file TFTP load requests
nvram:   Allow URL file TFTP load requests
system:  Allow URL file TFTP load requests

Router(config)# tftp-server
Router(config)# tftp-server flash:?
flash:c2500-jos56i-l.120-9.bin

Router(config)# tftp-server flash:c2500-jos56i-l.120-9.bin
Router(config)# ^Z
Router#
```

Step 3 After the TFTP server is configured, you can download the specified image from the router using the **copy tftp flash** command, as if it were a classic TFTP server.

Note The IP address of your TFTP server is the address of the router on which you configured the **tftp-server** command.

# Resolving Common Image Installation Problems

Note The information in this document is based on Cisco IOS Release 11.2 and later releases.

This appendix is designed to assist you with problems that may develop while you are installing Cisco IOS software images using a TFTP or remote copy protocol (rcp) server application. For rcp applications, substitute rcp for TFTP in the instructions.

## Before You Begin

Caution Do not save anything while you are in boot mode. Avoid using the saving commands (**write mem** or **copy run start**), and respond **no** to any prompt suggesting that you save your current configuration. If you save while you are in this mode, your configuration can be partially or completely erased.

## Resolving Default Gateway Issues

### Determining the Default Gateway for the Router

The default gateway is always the next hop that any packet will have to cross to reach the workstation where you have the TFTP server or Telnet session source, or both. The **traceroute** command shows the IP address of the default gateway in the first line of the output:

Example

```
Router> traceroute 172.17.247.195

Type escape sequence to abort.
Tracing the route to 172.17.247.195

1 10.200.40.1 4 msec 4 msec 4 msec
2 172.17.247.195 4 msec *  0 msec

Router>
```

## Adding the Default Gateway in the Configuration

To add the default gateway, type the **ip default-gateway** command in the global configuration mode:

```
ip default-gateway [ip address]
```

| Syntax Description | | |
|---|---|---|
| | `ip address` | The IP address of the router. |

## Verifying the TFTP Server and Router are in the Same Network

You will need to compare the IP addresses and masks of the TFTP server and the Ethernet interface of the router.

### Example 1

The TFTP server IP address is 172.17.247.195 and the mask is 255.255.0.0. The interface Ethernet 0 of the router IP address is 172.17.3.192 and the mask is 255.255.0.0. In this example, the TFTP server and this interface of the router are in the same network, so a default gateway is not required.

### Example 2

The TFTP server IP address is 172.17.247.195 and the mask is 255.255.0.0. The interface Ethernet 0 of the router IP address is 172.10.3.192 and the mask is 255.255.0.0. In this example, they are on different IP networks so it is necessary to configure a default gateway on the router.

## Determining the IP Address and Mask on the Router

Look for the IP address command under the interface Ethernet statement in your configuration.

### Example

```
Router> en
Password:
Router# show run
Building configuration...

Current configuration:
!
version 11.3
service timestamps debug uptime

...................

interface Ethernet0
ip address 172.17.3.192 255.255.0.0
```

### Determining the IP Address of the TFTP Server on Windows 95

Step 1 From the toolbar, select **Start** and then **Run**.

Step 2 Type **winipcfg** and then click **OK** to display the IP configuration dialog box.

### Determining the IP Address of the TFTP Server on a UNIX Workstation

Step 1 Enter the command **netstat -in**. The IP addresses of the interfaces on your station appear.

Step 2 Select the IP address for the interface that goes into the router network.

## Troubleshooting Problems During Software Transfer

### Resolving Error Message "Text checksum verification failure" During the Copy

If you have seen many "." instead of "!" during the copy, you may see a message similar to the following example:

```
COPY: Text checksum verification failure
TFTP from 172.17.247.195 failed/aborted
Verifying checksum... invalid (expected 0x62B7,
computed 0x60B9)
```

If you enter a **show flash** command, you may see something similar to the following example:

```
Router# show flash
PCMCIA flash directory:
File Length Name/status
1 3437967 c1600-sy-mz.120-8.0.2.T
2 3489036 c1600-y-l.112-19.P1
3 290304 c1600-y-l.112-18.P [invalid checksum]
```

In both cases, a checksum failure indicates that the file has not been properly copied into the memory and you need to copy it again. First, verify that the file you copied to the TFTP server is the same size as the original file. (Be aware that the size is listed in bytes in the router and is sometimes listed in kilobytes in TFTP servers.) If the network is very busy, you may also see this behavior; try the copy again when the network is not so loaded, or establish a direct Ethernet connection between the TFTP server and the router to download the file.

### Resolving Error Message "error opening tftp"

This is an example of the error message:

```
Router# copy tftp flash
Address or name of remote host [172.17.0.5]?
Source filename [rsp-dsv-mz.112-19.P1.bin]?
Destination filename [rsp-dsv-mz.112-19.P1.bin]?
Accessing tftp://172.17.0.5/rsp-dsv-mz.112-19.P1.bin...
%Error opening tftp://172.17.0.5/rsp-dsv-mz.112-19.P1.bin (No such file or directory)
```

If you receive this message, verify that the file is in the root directory of the TFTP server, and check to see if you entered the correct filename. Some easily mistaken letters are I (capital i), l (small L) and 1 (one).

## Resolving Display of Timeout Error Messages

Step 1 Verify that the TFTP server is open on your PC.

Step 2 Make sure that the file is in the root directory (from the menu bar, select **View**>**Options**).

## Resolving Error Message "Can't open file"

Verify that the TFTP server is running on your PC. Verify that you have copied the exact filename. Some easily mistaken letters are I (capital i), l (small L) and 1 (one).

### Instructions for Run-from-RAM Installations

Step 1 To copy a system image from one device to another, use the **copy** command in global configuration mode.

```
copy tftp ?
```

Step 2 Refer to the *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.2 for additional information about the **copy** command. Methods vary according to different platforms.

The three most common forms of the **copy** command for this purpose are as follows:

```
copy tftp flash
copy rcp flash
copy slot0: slot1:
```

The following example provides an illustration of the **copy slot0: slot1** command:

```
router# show slot0:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------
name
1 .D unknown 5E8B84E6 209D8 11 2392 Jan 22 2000 00:22:42
flashconfig
2 .. image 5E7BAE19 B623C4 22 11802988 Jan 22 2000 00:23:18
rsp-jsv-mz.1
20-8.0.2.T

router# show slot1:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------
name
1 .. unknown 6A2B4BA7 6FA9E0 20 7186784 Jul 30 1999 15:05:19
rsp-jv-mz.11 1-26.CC1
2 .. config 631F0D8B 6FB1EC 6 1929 Oct 19 1999 06:15:49
config
     3 .. config 631F0D8B 6FB9F8 7 1929 Oct 19 1999 06:16:03
     config1

router# copy slot0: slot1:
Source filename []? rsp-jsv-mz.120-8.0.2.T
```

```
Destination [slot1]?
CCCCCCCCCCCCCCCCCCC
2392 bytes copied in 0.300 secs
```

### Instructions Before Reloading

Step 1 Verify that the new Cisco IOS software image has been stored properly. Use the **show flash** command to make sure that the file has been saved, that the size is correct, and that you do not have an invalid checksum message.

If the file does not appear, or if it appears followed by "[invalid checksum]", or if the size does not correspond to the file size on the tftp server, you must start the installation again. Be aware that the size is listed in bytes in the router and is sometimes listed in kilobytes in TFTP servers.

Step 2 Verify that the boot system commands are in the right order in the configuration. The router stores and executes the **boot system** commands in the order in which you enter them in the configuration file. If a **boot system** command entry in the list specifies an invalid device or filename, the router skips that entry.

This is an example of **boot system** commands defined in the configuration file:

```
Router> en
Password:
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)# boot system flash c1600-y-l.112-18.P
Router(config)# boot system flash
```

# Troubleshooting Problems by Verifying the Software Image

## Resolving the show version Command not Displaying Proper Image

If the **show version** command output does not display the Cisco IOS image that you just loaded, perform these steps:

Step 1 Verify that the new Cisco IOS software image has been stored properly. Use the **show flash** command to make sure that the file has been saved, that the size is correct, and that you do not have an invalid checksum message.

If the file does not appear, or if it appears followed by "[invalid checksum]", or if the size does not correspond to the file size on the tftp server, you need to start the installation again. Be aware that the size is listed in bytes in the router and is sometimes listed in kbytes in TFTP servers.

Step 2 Verify that the boot system commands are in the right order in the configuration. The router stores and executes the **boot system** commands in the order in which you enter them in the configuration file. If a **boot system** command entry in the list specifies an invalid device or filename, the router skips that entry.

## Resolving the Rxboot Prompt (Router(boot)>) Displaying After Reload

Step 1 Verify that the new Cisco IOS software image has been stored properly. Use the **show flash** command to make sure that the file has been saved, that the size is correct, and that you do not have an invalid checksum message.

If the file does not appear, or if it appears followed by "[invalid checksum]", or if the size does not correspond to the file size on the tftp server, you need to start the installation again. Be aware that the size is listed in bytes in the router and is sometimes listed in kbytes in TFTP servers.

Step 2 Verify that the boot system commands are in the right order in the configuration. The router stores and executes the **boot system** commands in the order in which you enter them in the configuration file. If a **boot system** command entry in the list specifies an invalid device or filename, the router skips that entry.

Step 3 Verify that the config register value is correct. The last digit should be a 2. You can check this with the **show version** command. If the value is not correct, you need to restore a valid value and reload the image.

## Related Information

- *Router and IOS Architecture Technical Tips*
- *Release Notes for the Cisco uBR7200 Series* web page

# Viewing Sample Configuration Files

This appendix contains examples of Cisco uBR7200 series universal broadband router configuration files. To view the current configuration of a Cisco uBR7200 series router, enter the **show running-config** command at the CLI prompt in EXEC mode or privileged EXEC mode.

## Basic Internet Access Examples

### General Example

This section provides a Cisco Release 12.0(5)T sample configuration file for the Cisco uBR7246, including spectrum management and modulation profile configuration for QAM 16:

```
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uBR7246
!
boot system flash slot0:ubr7200-p-mz.120-5.T
boot system flash
!
cable spectrum-group 1 frequency 40000000
cable spectrum-group 1 frequency 20000000 2
cable modulation-profile 3 request 0 16 1 8 16qam scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 3 initial 5 34 0 48 16qam scrambler 152 no-diff 256 fixed uw16
cable modulation-profile 3 station 5 34 0 48 16qam scrambler 152 no-diff 256 fixed uw16
cable modulation-profile 3 short 5 75 6 8 16qam scrambler 152 no-diff 144 fixed uw8
cable modulation-profile 3 long 8 220 0 8 16qam scrambler 152 no-diff 160 fixed uw8
no cable qos permission create
no cable qos permission update
cable qos permission modems
ip subnet-zero
ip dhcp relay information option
!
interface FastEthernet0/0
ip address 10.1.70.2 255.255.255.0
no ip directed-broadcast
no ip mroute-cache
!
!
interface Ethernet2/3
ip address 1.3.59.1 255.255.0.0
```

```
no ip directed-broadcast
!
interface Cable5/0
ip address 172.1.71.1 255.255.255.0 secondary
ip address 10.1.71.1 255.255.252.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no keepalive
no cable proxy-arp

cable helper-address 10.1.70.30
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable upstream 0 spectrum-group 1
cable upstream 0 modulation-profile 3
cable downstream frequency 531000000
cable upstream 0 frequency 28000000
cable upstream 0 power-level 0
no cable upstream 0 shutdown
cable upstream 1 shutdown
cable upstream 2 shutdown
cable upstream 3 shutdown
cable upstream 4 shutdown
cable upstream 5 shutdown
!
!
router eigrp 100
network 10.0.0.0
!
ip classless
no ip http server
!
!
!
line con 0
password cisco
login
transport input none
line aux 0
line vty 0 4
password cisco
login
!
end
```

The command lines in the sample configuration file beginning with the string **cable spectrum-group** contain the critical elements necessary to set up spectrum management in your overall configuration:

```
cable spectrum-group 1 frequency 40000000
cable spectrum-group 1 frequency 20000000 2
```

In this case, the user has configured spectrum management group number “1” to be available to upstream channels. As defined by the two command lines above, the “preferred” choice is for the upstream to operate on a 40 MHz channel. If that channel is not suitable for the transmission scheme available, the upstream will automatically move over to transmitting at 20 MHz and increase the receive power rating by 2 dB.

The command lines in the sample configuration file beginning with the string **cable modulation-profile** contain the critical elements necessary to set up a modulation profile in your overall configuration:

```
cable modulation-profile 3 request 0 16 1 8 16qam scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 3 initial 5 34 0 48 16qam scrambler 152 no-diff 256 fixed uw16
cable modulation-profile 3 station 5 34 0 48 16qam scrambler 152 no-diff 256 fixed uw16
cable modulation-profile 3 short 5 75 6 8 16qam scrambler 152 no-diff 144 fixed uw8
cable modulation-profile 3 long 8 220 0 8 16qam scrambler 152 no-diff 160 fixed uw8
```

In this case, the user has configured modulation profile number “3” to be available to upstream channels wherever they are configured to apply it. Note that this modulation profile has been configured to operate with a 16 QAM modulation scheme. The default modulation scheme for any upstream profile (if it is not set to 16 QAM) is QPSK.

Later in the configuration file example, upstream port 0 on the cable modem card installed in slot 5 utilizes both the spectrum management and the modulation profile configured in the sample.

```
cable upstream 0 spectrum-group 1
cable upstream 0 modulation-profile 3
```

This section provides a Cisco Release 12.0(8)SC sample configuration file, showing roughly the same capabilities as in the Cisco IOS Release 12.0(5)T image:

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname newtown01-7246
!
boot system flash slot0:ubr7200-k1ps-mz.120-8.SC.bin
boot system flash slot0:
boot config slot0:C7246
boot bootldr slot0:ubr7200-boot-mz.120-8.SC.bin
enable secret 5 <removed>
enable password 7 <removed>
!
cable flap-list size 4000
cable flap-list power-adjust threshold 3
cable flap-list aging 86400
cable spectrum-group 1 hop threshold 15
cable spectrum-group 1 frequency 26000000
cable spectrum-group 1 frequency 24000000 1
cable spectrum-group 1 frequency 22000000 2
no cable qos permission create
no cable qos permission update
cable qos permission modems
!
!
!
!
clock timezone GMT 0
ip subnet-zero
no ip source-route
no ip finger
ip telnet source-interface FastEthernet0/0
!
!
!
interface FastEthernet0/0
ip address 10.0.0.1 255.255.255.0 secondary
ip address 209.187.212.2 255.255.255.252
no ip directed-broadcast
no ip mroute-cache
full-duplex
no cdp enable
!
```

```
interface Cable3/0
description Sunnyvale, CA
ip address 209.187.213.1 255.255.255.0 secondary
ip address 10.8.0.1 255.255.0.0
no ip directed-broadcast
no ip mroute-cache
no keepalive
cable spectrum-group 1
cable dhcp-giaddr policy
cable helper-address 209.187.212.12
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream frequency 687000000
cable upstream 0 description Sunnyvale 1-5
cable upstream 0 power-level 0
no cable upstream 0 shutdown
cable upstream 1 description Sunnyvale 6-10
cable upstream 1 power-level 0
no cable upstream 1 shutdown
cable upstream 2 description Sunnyvale 1-6
cable upstream 2 power-level 0
no cable upstream 2 shutdown
cable upstream 3 description Sunnyvale 7-11
cable upstream 3 power-level 0
no cable upstream 3 shutdown
cable upstream 4 description Sunnyvale 12-17
cable upstream 4 power-level 0
no cable upstream 4 shutdown
cable upstream 5 description Sunnyvale 18-23
cable upstream 5 power-level 0
no cable upstream 5 shutdown
!
interface Cable4/0
description Santa Clara, CA
ip address 207.252.148.1 255.255.255.0 secondary
ip address 10.9.0.1 255.255.0.0
no ip directed-broadcast
no ip mroute-cache
no keepalive
cable spectrum-group 1
cable dhcp-giaddr policy
cable helper-address 209.187.212.12
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream frequency 687000000
cable upstream 0 description Santa Clara 1-8
cable upstream 0 power-level 0
cable upstream 0 shutdown
cable upstream 1 description Santa Clara 1-7
cable upstream 1 power-level 0
no cable upstream 1 shutdown
cable upstream 2 description Santa Clara 8-13
cable upstream 2 power-level 0
no cable upstream 2 shutdown
cable upstream 3 description Santa Clara14-19
cable upstream 3 power-level 0
no cable upstream 3 shutdown
able upstream 4 description Santa Clara 20-26
cable upstream 4 power-level 0
no cable upstream 4 shutdown
cable upstream 5 description Santa Clara 27-33
cable upstream 5 power-level 0
```

```
no cable upstream 5 shutdown
!
interface Cable5/0
description San Jose, CA
ip address 207.252.149.1 255.255.255.0 secondary
ip address 10.10.0.1 255.255.0.0
no ip directed-broadcast
no ip mroute-cache
no keepalive
cable spectrum-group 1
cable dhcp-giaddr policy
cable helper-address 209.187.212.12
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream frequency 687000000
cable upstream 0 description Willow Glen 1-8
cable upstream 0 power-level 0
no cable upstream 0 shutdown
cable upstream 1 description Willow Glen 9-16
cable upstream 1 power-level 0
no cable upstream 1 shutdown
cable upstream 2 description Willow Glen 17-24
cable upstream 2 power-level 0
no cable upstream 2 shutdown
cable upstream 3 description Willow Glen 25-32
cable upstream 3 power-level 0
no cable upstream 3 shutdown
cable upstream 4 description Evergreen 1-8
cable upstream 4 power-level 0
no cable upstream 4 shutdown
able upstream 5 description Evergreen 9-17
cable upstream 5 power-level 0
no cable upstream 5 shutdown
!
interface Cable6/0
description Morgan Hill, CA
ip address 209.187.214.1 255.255.255.0 secondary
ip address 10.11.0.1 255.255.0.0
no ip directed-broadcast
no ip mroute-cache
no keepalive
cable spectrum-group 1
cable dhcp-giaddr policy
cable helper-address 209.187.212.12
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream frequency 687000000
cable upstream 0 description Santa Theresa 1-5
cable upstream 0 power-level 0
cable upstream 0 shutdown
cable upstream 1 description Santa Theresa 6-10
cable upstream 1 power-level 0
cable upstream 1 shutdown
cable upstream 2 description Santa Theresa 11-14
cable upstream 2 power-level 0
cable upstream 2 shutdown
cable upstream 3 description Santa Theresa 1-5
cable upstream 3 power-level 0
no cable upstream 3 shutdown
cable upstream 4 description Santa Theresa 6-11
cable upstream 4 power-level 0
no cable upstream 4 shutdown
```

```
cable upstream 5 description Santa Theresa 12-17
cable upstream 5 power-level 0
no cable upstream 5 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.187.212.1
ip route 0.0.0.0 0.0.0.0 Null0 255
!
> no cdp run
> snmp-server engineID local 000000090200003019OE0900
snmp-server community <removed> RO
snmp-server location San Jose, CA
snmp-server contact Jim Smith
snmp-server chassis-id 01
!
banner login ^C Warning!  Unauthorized use of this system is prohibited. =
You will be prosecuted to the fullest extent of =
the law.^C
alias exec qos show cable qos profile
alias exec scm show cable modem
alias exec noise show cable modem detail
!
line con 0
transport input none
line aux 0
line vty 0 4
exec-timeout 0 0
password 7 <removed>
login
!
ntp clock-period 17179915
ntp update-calendar
ntp max-associations 2000
ntp server 129.7.1.66 source FastEthernet0/0 prefer
end
```

## Baseline Privacy Interface Example

The Cisco uBR7200 series supports 56-bit and 40-bit encryption/decryption; 56 bit is the default. After you choose a CMTS image that supports BPI, BPI is enabled by default for the Cisco uBR7200 series. Key commands that appear in the Cisco uBR7200 series configuration file that denote encryption/decryption is supported include:

```
int cable 2/0
cable privacy kek grace-time 800
cable privacy kek life-time 750000
cable privacy tek grace-time 800
cable privacy tek life-time 56000
cable privacy enable
cable privacy mandatory
```

Note The cable modem must also support encryption/decryption.

When baseline privacy is enabled, the Cisco uBR7200 series routes encrypted/decrypted packets from a host or peer to another host or peer. BPI is configured with key encryption keys (keks) and traffic encryption keys (teks). A kek is assigned to a CM based on the CM's service identifier (SID) and permits the CM to connect to the Cisco uBR7200 series router when baseline privacy is activated. The tek is assigned to a CM when its kek has been established. The tek is used to encrypt data traffic between the CM and the Cisco uBR7200 series router.

Keks and teks can be set to expire based on a gracetime or a lifetime value. A gracetime key is used to assign a temporary key to a CM to access the network. A lifetime key is used to assign a more permanent key to a CM. Each CM that has a lifetime key assigned will request a new lifetime key from the Cisco uBR7200 series router before the current one expires.

Tip Use the **show cable modem** command to identify a CM with encryption/decryption enabled. The *online(pk)* output of this command reveals a CM that is registered with BPI enabled and a KEK assigned. The *online(pt)* output reveals a CM that is registered with BPI enabled and a TEK assigned.

Should you want to change the Cisco uBR7200 series default of 56-bit encryption/decryption to 40-bit, use the "40-bit-des" option:

```
CMTS(config-if)#cable privacy ?
  40-bit-des           select 40 bit DES
  ^^^^^^^^^^
  authenticate-modem   turn on BPI modem authentication
  authorize-multicast  turn on BPI multicast authorization
  kek                  KEK Key Parms
  mandatory            force privacy be mandatory
  tek                  TEK Key Parms
```

Software then generates a 40-bit DES key, where the DES key that is generated and returned masks the first 16-bits of the 56-bit key to zero in software. To return to 56-bit encryption/decryption after changing to 40-bit, enter the **no** command preceding the "40-bit-des" option.

Caution Cisco uBR7200 series telco return images that support BPI, do not support encryption/decryption in the telco return path.

## Euro-DOCSIS Operation Example

The Cisco uBR7200 series supports Euro-DOCSIS channel plans when using the MC16E cable interface line card. Key commands that appear in the Cisco uBR7200 series configuration file that denote Euro-DOCSIS operation include:

- **cable downstream annex A**—Annex A is reserved for Euro-DOCSIS operations (Annex B is used for DOCSIS NTSC operations). Annex A is chosen by default when using the MC16E.
- **cable upstream 0 frequency <5008000>**—The Euro-DOCSIS upstream valid range is from 5,000,000 to 65,000,000 Hz. You choose the value here.

Note The following Cisco IOS releases support Euro-DOCSIS operation using the MC16E cable interface line card: 12.0(7)T, 12.0(7)XR2, 12.1 Mainline, 12.1(1a)T1 and higher;
SC train images including 12.0(8)SC, 12.0(9)SC, and higher.

Tip In contrast to other cable interface line cards where you set the downstream modulation and interleave depth, the downstream interleave value is fixed for the MC16E and cannot be configured. The MC16E also does not support enhanced spectrum management.

A sample Euro-DOCSIS configuration file follows:

```
!
```

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R7732-06-uBR7246-CE
!
!
cable modulation-profile 1 request 0 16 1 8 16qam scrambler 152
no-diff 128 fixed uw16
cable modulation-profile 1 initial 5 34 0 48 16qam scrambler 152
no-diff 256 fixed uw16
cable modulation-profile 1 station 5 34 0 48 16qam scrambler 152
no-diff 256 fixed uw16
cable modulation-profile 1 short 6 75 6 8 16qam scrambler 152 no-diff
144 fixeduw8
cable modulation-profile 1 long 8 220 0 8 16qam scrambler 152 no-diff
160 fixeduw8
cable modulation-profile 2 request 0 16 1 8 qpsk scrambler 152 no-diff
64 fixeduw8
cable modulation-profile 2 initial 5 34 0 48 qpsk scrambler 152
no-diff 128 fixed uw16
cable modulation-profile 2 station 5 34 0 48 qpsk scrambler 152
no-diff 128 fixed uw16
cable modulation-profile 2 short 5 75 6 8 qpsk scrambler 152 no-diff
72 fixed uw8
cable modulation-profile 2 long 8 220 0 8 qpsk scrambler 152 no-diff
80 fixed uw8
!
no cable qos permission create
no cable qos permission update
cable qos permission modems
!
!
!
!
ip subnet-zero
ip host abrick 223.255.254.254
!
!
!
interface Loopback0
 ip address 222.2.4.1 255.255.255.255
 no ip directed-broadcast
!
interface Loopback2
 ip address 111.0.4.2 255.255.255.255
 no ip directed-broadcast
!
interface FastEthernet0/0
 ip address 1.8.93.9 255.255.0.0
 no ip directed-broadcast
!
interface Cable3/0
 ip address 3.214.1.1 255.255.255.0
 no ip directed-broadcast
 load-interval 30
 no keepalive
 cable spectrum-group 1
 cable helper-address 1.8.93.100
cable downstream annex A
 cable downstream modulation 64qam
 cable downstream frequency 669000000
cable upstream 0 frequency 5008000
```

```
 cable upstream 0 power-level 0
 no cable upstream 0 shutdown
 cable upstream 1 frequency 10000000
 cable upstream 1 power-level 0
 no cable upstream 1 shutdown
 cable upstream 2 frequency 15008000
 cable upstream 2 power-level 0
 no cable upstream 2 shutdown
 cable upstream 3 frequency 20000000
 cable upstream 3 power-level 0
 no cable upstream 3 shutdown
 cable upstream 4 frequency 55008000
 cable upstream 4 power-level 0
 no cable upstream 4 shutdown
 cable upstream 5 frequency 60000000
 cable upstream 5 power-level 0
 no cable upstream 5 shutdown
!
ip default-gateway 1.8.0.1
ip classless
ip route 223.255.254.254 255.255.255.255 1.8.0.1
!
snmp-server engineID local 00000009020000D0BA1EED00
snmp-server community public RO
snmp-server community private RW
!
alias exec scm show cable modem
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 password lab
 login
!
end
```

# Virtual Private Network (VPN) Example

VPN features let MSOs and ISPs offer private network connections to telecommuters and other business-oriented customers. In the configuration example that follows, a VPN is set up between two termination points:

- One at a remote cable modem
- The other at a VPN gateway residing at a corporate office firewall

Tip To properly transmit and receive encrypted/decrypted traffic, each peer in the VPN must activate encryption/decryption and have matching access key strings.

Note The Cisco uBR7200 series allows encrypted traffic to pass over the cable network (and often the Internet) from one peer to the other, based on a routing table setup in its configuration file.

## GRE Tunnel Example

In the example that follows, a Cisco uBR7200 series connects two branch office networks to their respective head office using a GRE tunnel.

Note Each branch office network is connected to the Cisco uBR7200 series using the cable interface. Each customer is assigned a separate subinterface over the physical cable interface.

The cable interface number 3 has been configured with two subinterfaces. Each subinterface connects to a customer Small Office Home Office (SOHO) CM:

```
!
interface Cable3/0
  no ip address
  no ip directed broadcasr
  no keepalive
  ip route-cache policy
!(To configure policy based route-cache on subinterfaces. This command not available on
subinterfaces.)
  cable downstream annex B
  cable downstream modulation 64qam
  cable downstream interleave-depth 32
  cable upstream 0 power-level 0
  no cable upstream 0 shutdown
!(While configuring the physical interface IP address and IP helper address parameters
must not be entered.)
interface c3/0.1
  ip address 172.100.1.1 255.255.255.0
  cable helper address 11.0.0.2
  ip policy route-map customer1
  no ip directed-broadcast
  no cable proxy-arp
  no cable ip-multicast-echo

interface c3/0.2
  ip address 174.100.1.1 255.255.255.0
  ip helper address 11.0.0.2
  ip policy route-map customer2
  no ip directed-broadcast
  no cable proxy-arp
  no cable ip-multicast-echo

interface serial 0
  ip address 151.145.1.1 255.255.255.0
interface tunnel 0
  ip address 172.100.3.1 255.255.255.252
  tunnel source s0
  tunnel destination 151.145.2.1

interface tunnel 1
  ip address 174.100.3.1 255.255.252
  tunnel source s0
  tunnel destination 151.145.3.1

! configure route maps to forward traffic coming over c3/0.1 and c3/0.2 to go over the
tunnel 0 and
! tunnel 1 respectively.
route-map customer1 permit 10
  match ip address 101
   set ip next-hop 11.1.1.1
route-map customer1 permit 20
```

```
  match ip address 102
   set ip next-hop 172.100.3.2
route-map customer2 permit 10
  match ip address 101
   set ip next-hop 11.1.1.1
!(traffic to go over the interface that connects to DHCP/DNS/TFTP Server)
route-map customer2 permit 20
  match ip address 102
   set ip next-hop 174.100.3.2
access-list 101 permit ip any 11.1.1.0 0.0.0.255
!(matches traffic destined for DHCP/DNS/TFTP server)
access-list 102 permit ip any any
!(any other traffic that is not meant for DHCP/DNS/TFTP server)
ip route 151.145.0.0 255.255.0.0 s0 <- static route to connect to IP Cloud.
```

Note You can use **set ip default next-hop a.b.c.d** to avoid setting up two access lists. The access list can match all IP traffic and the **route-map** command should use **set ip default next-hop a.b.c.d.** This works with CEF and process switching, not with cache-based fast switching. The packets are first routed normally using the routing table. If a route is not found, then they are forwarded to **a.b.c.d** which is the IP address at the other end of the tunnel.

### Configuration for Router #1

```
interface ethernet0
  ip address 172.100.2.1 255.255.255.0

interface serial 0
  ip address 151.145.2.1 255.255.255.0

interface tunnel 0
  ip address 172.100.3.2 255.255.255.252
  tunnel source s0
  tunnel destination 151.145.1.1

ip route 151.145.0.0 255.255.0.0 s0
!(static route to connect to IP Cloud)
```

### Configuration for Router #2

```
interface ethernet0
  ip address 174.100.2.1 255.255.255.0
interface serial 0
  ip address 151.145.3.1 255.255.255.0
interface tunnel 0
  ip address 174.100.3.2 255.255.255.252
  tunnel source s0
  tunnel destination 151.145.1.1
ip route 151.145.0.0 255.255.0.0 s0
!(static route to connect to IP Cloud)
exec-timeout 0 0
 login
 transport input none
line aux 0
line vty 0 4
 password lab
 login
!
scheduler allocate 988 200
end
```

# IP Telephony Example

## General Example

To support IP telephony, a cable modem supporting VoIP communications must reside at the subscriber site.

**Caution** In certain countries, the provisioning of voice telephony over the Internet or use of these products might be prohibited and/or subject to laws, regulations or licenses, including requirements applicable to the use of the products under telecommunications and other laws and regulations; customers must comply with all such applicable laws in the countries where customers intend to use the product.

Following is a sample voice over IP configuration file for the Cisco uBR7246:

```
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname twoslot
!
enable password ****
!
!
ip subnet-zero
no ip domain-lookup
ip host abrick 223.255.254.254
ip host muck 255.255.255.255
ip host keyer 223.255.254.254
ip host bell 223.255.254.253
!
!
!
interface FastEthernet0/0
ip address 2.2.2.2 255.255.255.0
no ip directed-broadcast
no ip mroute-cache
shutdown
!
interface Ethernet1/0
ip address 1.11.8.1 255.255.0.0
ip broadcast-address 1.11.255.255
ip helper-address 223.255.254.254
no ip directed-broadcast
no ip mroute-cache
!
interface Ethernet1/1
ip address 10.20.122.2 255.255.255.192
ip helper-address 10.0.0.2
no ip directed-broadcast
!
interface Ethernet1/2
no ip address
no ip directed-broadcast
shutdown
!
interface Ethernet1/3
```

```
no ip address
no ip directed-broadcast
shutdown
!
interface Cable2/0
ip address 20.20.20.20 255.255.255.0
no ip directed-broadcast
no keepalive
cable downstream modulation 64qam
cable upstream 0 frequency 10000000
cable upstream 0 power-level 0
no cable upstream 0 shutdown
cable upstream 1 frequency 10000000
cable upstream 1 power-level 0
no cable upstream 1 shutdown
cable upstream 2 shutdown
cable upstream 3 shutdown
cable upstream 4 shutdown
cable upstream 5 shutdown
!
ip default-gateway 1.11.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.20.122.1
ip route 223.255.254.254 255.255.255.255 1.11.0.1
ip http server
!
!
!
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
login
line vty 5 11
login
!
end
```

## Clock Support Example

Clock support enables the Cisco uBR7246 VXR router to synchronize to an external timing reference and distribute clock to Cisco MC16S and MC16E cable interface line cards. The synchronized DOCSIS time stamps are then passed downstream to all CMs.

Note Clock support is designed for cable networks running VoIP applications where synchronized timing is vital to maintain voice quality. The clocking feature is supported only on a Cisco uBR7246 VXR chassis that contains the clock card and uses Cisco IOS Release 12.1(1a)T1 or higher. The CM must also support VoIP and the clock mode.

Tip No configuration tasks are required to use the clock card after it is installed in the Cisco uBR7246 VXR. When the clock card is present, it becomes the midplane TDM clock reference source.

Key commands that appear in the Cisco uBR7246 VXR configuration file that denote clock support include:

```
cable clock source-midplane
no cable clock force primary
no cable clock force secondary
```

## Telco Return Example

Cisco IOS Release CMTS software images that support telco return contain a "t" in the file name. To support telco return, a DOCSIS-compliant telco return cable modem must reside at the subscriber site and support the telco return path.

Verify whether or not the cable modem requires the following setup:

- Dial-on-demand functionality; include the **cable telco-return spd** *number* **dial-timer** *seconds* command in the Cisco uBR7200 series configuration file. This command embeds dial-timer information in the TCD messages that are sent regularly to the remote cable modem which ultimately cuts-off any inactive upstream connections.
- Cisco Network Registrar setup to service both telco return and two-way cable modems over the same downstream channel.

Note Some vendors' telco return cable modems cannot receive traffic over the same downstream channel as cable modems operating on a two-way data system. In these instances, segment your cable plant to allow more than one downstream channel.

The following elements must be configured for a telco return network:

- Authentication, authorization, and accounting configuration, as well as specific RADIUS dial server information
- Telco return-specific configuration
- SNMP server-specific configuration

This sample Cisco uBR7200 series configuration file supports telco return:

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname uBR7246
!
boot system flash slot0:ubr7200-p-mz.**********
boot system flash
logging buffered 100000 debugging
aaa new-model
aaa authentication login default radius enable
aaa authentication login vty line
aaa accounting update newinfo
aaa accounting exec default start-stop radius
aaa accounting commands 15 default start-stop radius
aaa accounting network default start-stop radius
aaa accounting system default start-stop radius
enable secret guess_my_password_ha_ha_ha.
!
no cable qos permission create
no cable qos permission update
cable qos permission modems
ip subnet-zero
```

```
no ip finger
no ip domain-lookup
!
!
!
interface Loopback0
ip address 24.1.2.246 255.255.255.0
no ip directed-broadcast
!
interface FastEthernet0/0
no ip address
no ip directed-broadcast
shutdown
media-type MII
full-duplex
!
interface Hssi1/0
ip unnumbered Loopback0
no ip directed-broadcast
!
interface Cable3/0
ip address 10.1.1.1 255.255.255.0
no ip directed-broadcast
cable helper-address 24.1.1.84
no keepalive
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream frequency 687000000
cable upstream 0 frequency 13008000
no cable upstream 0 shutdown
cable upstream 1 shutdown
cable upstream 2 shutdown
cable upstream 3 shutdown
cable upstream 4 shutdown
cable upstream 5 shutdown
!
interface Cable6/0
ip address 172.16.1.1 secondary
ip address 10.1.1.1
no ip directed-broadcast
cable helper-address 24.1.1.84
no keepalive
cable downstream annex B
cable downstream modulation 64qam
cable downstream interleave-depth 32
cable downstream frequency 687000000
cable upstream 0 frequency 13008000
no cable upstream 0 shutdown
cable telco-return enable
cable telco-return spd 1 factory-default
cable telco-return spd 1 dhcp-authenticate
cable telco-return spd 1 dhcp-server 24.1.1.84
cable telco-return spd 1 ppp-authenticate chap
cable telco-return spd 1 phonenum 918005555555
cable telco-return spd 1 phonenum 18005555555
cable telco-return spd 1 username test
cable telco-return spd 1 password test
!
router ospf 100
network 10.0.0.0 0.255.255.255 area 0
network 24.1.0.0 0.0.255.255 area 0
!
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 24.1.2.21
!
logging 24.1.1.78
snmp-server community public RO
snmp-server community favorite_server_community RW
snmp-server location favorite_location
!
radius-server host 24.1.1.78 auth-port 1645 acct-port 1646
radius-server key radius_server_key
!
line con 0
password No need to change; this is encrypted already.
transport input none
flowcontrol software
line aux 0
password No need to change; this is encrypted already.
flowcontrol hardware
line vty 0 4
password No need to change; this is encrypted already.
login authentication vty
!
end
```

The command lines in the sample configuration file beginning with the string **aaa** contain the critical elements for authentication, authorization, and accounting (AAA) setup:

```
aaa new-model
aaa authentication login default radius enable
aaa authentication login vty line
aaa accounting update newinfo
aaa accounting exec default start-stop radius
aaa accounting commands 15 default start-stop radius
aaa accounting network default start-stop radius
aaa accounting system default start-stop radius
```

The command lines in the sample configuration file beginning with the string **cable telco-return** contain the critical elements to minimally set up the telco return network:

```
cable telco-return enable
cable telco-return spd 1 factory-default
cable telco-return spd 1 dhcp-authenticate
cable telco-return spd 1 dhcp-server 24.1.1.84
cable telco-return spd 1 ppp-authenticate chap
cable telco-return spd 1 phonenum 918005555555
cable telco-return spd 1 phonenum 18005555555
cable telco-return spd 1 username test
cable telco-return spd 1 password test
```

First, activate telco return functionality with the **enable** keyword. Then activate DHCP authentication and identify the location of the DHCP server, provide up to three telephone numbers for dial-in access, specify the type of PPP authentication for upstream transmission, and provide the user name and password to authorize login to the dial-up network.

Note PPP is the only upstream communication medium offered between a remote cable modem and a dial-up access server. You can, however, configure a Challenge Handshake Authentication Protocol (CHAP), or Password Authentication Protocol (PAP) authentication method, or both methods for upstream data transmission.

The command lines in the sample configuration file beginning with the string **snmp-server** contain the critical elements for minimal SNMP-server setup:

```
logging 24.1.1.78
snmp-server community public RO
snmp-server community favorite_server_community RW
snmp-server location favorite_location
```

The command lines in the sample configuration file beginning with the string **radius-server** contain the critical elements for minimal RADIUS dial server setup:

```
radius-server host 24.1.1.78 auth-port 1645 acct-port 1646
radius-server key radius_server_key
```

Note For more detailed information regarding AAA, telco return, SNMP server, and RADIUS dial server software functionality, you can access Cisco IOS software configuration documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

# Frequency Allocation for the Cisco uBR7200 Series Universal Broadband Routers

Table D-1 provides information on NTSC 6-MHz channel bands. Table D-2 provides information on the Phase Alternating Line (PAL) and Systeme Electronique Couleur Avec Memoire (SECAM) 8-MHz channel bands.

*Table D-1 NTSC Cable Television Channels and Relative Frequencies in MHz*

| Channel Number | Bandwidth | Video Carrier | Color Carrier | Audio Carrier |
|---|---|---|---|---|
| T 7 | 5.75 - 11.75 | 7 | 10.58 | 11.5 |
| T 8 | 11.75 - 17.75 | 13 | 16.58 | 17.5 |
| T9 | 17.75-23.75 | 19 | 22.58 | 23.5 |
| T10 | 23.75-29.75 | 25 | 28.58 | 29.5 |
| T11 | 29.75-35.75 | 31 | 34.58 | 35.5 |
| T12 | 35.75-41.75 | 37 | 40.58 | 41.5 |
| T13 | 41.75-47.75 | 43 | 46.58 | 47.5 |
| TV-IF | 40.0-46.0 | 45.75 | 42.17 | 41.25 |
| 2-2 | 54.0-60.0 | 55.25 | 58.83 | 59.75 |
| 3-3 | 60.0-66.0 | 61.25 | 64.83 | 65.75 |
| 4-4 | 66.0-72.0 | 67.25 | 70.83 | 71.75 |
| 5-5 | 76.0-82.0 | 77.25 | 80.83 | 81.75 |
| 6-6 | 82.0-88.0 | 83.25 | 86.83 | 87.75 |
| FM | 88.0-108.0 | | | |
| A-5-95 | 90.0-96.0 | 91.25 | 94.83 | 95.75 |
| A-4-96 | 96.0-102.0 | 97.25 | 100.83 | 101.75 |
| A-3-97 | 102.0-108.0 | 103.25 | 106.83 | 107.75 |
| A-2-98 | 108.0-114.0 | 109.25 | 112.83 | 113.75 |
| A-1-99 | 114.0-120.0 | 115.25 | 118.83 | 119.75 |
| A-14 | 120.0-126.0 | 121.25 | 124.83 | 125.75 |
| B-15 | 126.0-132.0 | 127.25 | 130.83 | 131.75 |
| C-16 | 132.0-138.0 | 133.25 | 136.83 | 137.75 |

*Table D-1 NTSC Cable Television Channels and Relative Frequencies in MHz (continued)*

| Channel Number | Bandwidth | Video Carrier | Color Carrier | Audio Carrier |
|---|---|---|---|---|
| D-17 | 138.0-144.0 | 139.25 | 142.83 | 143.75 |
| E-18 | 144.0-150.0 | 145.25 | 148.83 | 149.75 |
| F-19 | 150.0-156.0 | 151.25 | 154.83 | 155.75 |
| G-20 | 156.0-162.0 | 157.25 | 160.83 | 161.75 |
| H-21 | 162.0-168.0 | 163.25 | 166.83 | 167.75 |
| I-22 | 168.0-174.0 | 169.25 | 172.83 | 173.75 |
| 7-7 | 174.0-180.0 | 175.25 | 178.83 | 179.75 |
| 8-8 | 180.0-186.0 | 181.25 | 184.83 | 185.75 |
| 9-9 | 186.0-192.0 | 187.25 | 190.83 | 191.75 |
| 10-10 | 192.0-198.0 | 193.25 | 196.83 | 197.75 |
| 11-11 | 198.0-204.0 | 199.25 | 202.83 | 203.75 |
| 12-12 | 204.0-210.0 | 205.25 | 208.83 | 209.75 |
| 13-13 | 210.0-216.0 | 211.25 | 214.83 | 215.75 |
| J-23 | 216.0-222.0 | 217.25 | 220.83 | 221.75 |
| K-24 | 222.0-228.0 | 223.25 | 226.83 | 227.75 |
| L-25 | 228.0-234.0 | 229.25 | 232.83 | 233.75 |
| M-26 | 234.0-240.0 | 235.25 | 238.83 | 239.75 |
| N-27 | 240.0-246.0 | 241.25 | 244.83 | 245.75 |
| O-28 | 246.0-252.0 | 247.25 | 250.83 | 251.75 |
| P-29 | 252.0-258.0 | 253.25 | 256.83 | 257.75 |
| Q-30 | 258.0-264.0 | 259.25 | 262.83 | 263.75 |
| R-31 | 264.0-270.0 | 265.25 | 268.83 | 269.75 |
| S-32 | 270.0-276.0 | 271.25 | 274.83 | 275.75 |
| T-33 | 276.0-282.0 | 277.25 | 280.83 | 281.75 |
| U-34 | 282.0-288.0 | 283.25 | 286.83 | 287.75 |
| V-35 | 288.0-294.0 | 289.25 | 292.83 | 293.75 |
| W-36 | 294.0-300.0 | 295.25 | 298.83 | 299.75 |
| AA-37 | 300.0-306.0 | 301.25 | 304.83 | 305.75 |
| BB-38 | 306.0-312.0 | 307.25 | 310.83 | 311.75 |
| CC-39 | 312.0-318.0 | 313.25 | 316.83 | 317.75 |
| DD-40 | 318.0-324.0 | 319.25 | 322.83 | 323.75 |
| EE-41 | 324.0-330.0 | 325.25 | 328.83 | 329.75 |
| FF-42 | 330.0-336.0 | 331.25 | 334.83 | 335.75 |
| GG-43 | 336.0-342.0 | 337.25 | 340.83 | 341.75 |
| HH-44 | 342.0-348.0 | 343.25 | 346.83 | 347.75 |
| II-45 | 348.0-354.0 | 349.25 | 352.83 | 353.75 |

*Table D-1 NTSC Cable Television Channels and Relative Frequencies in MHz (continued)*

| Channel Number | Bandwidth | Video Carrier | Color Carrier | Audio Carrier |
|---|---|---|---|---|
| JJ-46 | 354.0-360.0 | 355.25 | 358.83 | 359.75 |
| KK-47 | 360.0-366.0 | 361.25 | 364.83 | 365.75 |
| LL-48 | 366.0-372.0 | 367.25 | 370.83 | 371.75 |
| MM-49 | 372.0-378.0 | 373.25 | 376.83 | 377.75 |
| NN-50 | 378.0-384.0 | 379.25 | 382.83 | 383.75 |
| OO-51 | 384.0-390.0 | 385.25 | 388.83 | 389.75 |
| PP-52 | 390.0-396.0 | 391.25 | 394.83 | 395.75 |
| QQ-53 | 396.0-402.0 | 397.25 | 400.83 | 401.75 |
| RR-54 | 402.0-408.0 | 403.25 | 406.83 | 407.75 |
| SS-55 | 408.0-414.0 | 409.25 | 412.83 | 413.75 |
| TT-56 | 414.0-420.0 | 415.25 | 418.83 | 419.75 |
| UU-57 | 420.0-426.0 | 421.25 | 424.83 | 425.75 |
| VV-58 | 426.0-432.0 | 427.25 | 430.83 | 431.75 |
| WW-59 | 432.0-438.0 | 433.25 | 436.83 | 437.75 |
| XX-60 | 438.0-444.0 | 439.25 | 442.83 | 443.75 |
| YY-61 | 444.0-450.0 | 445.25 | 448.83 | 449.75 |
| ZZ-62 | 450.0-456.0 | 451.25 | 454.83 | 455.75 |
| AAA-63 | 456.0-462.0 | 457.25 | 460.83 | 461.75 |
| BBB-64 | 462.0-468.0 | 463.25 | 466.83 | 467.75 |
| CCC-65 | 468.0-474.0 | 469.25 | 472.83 | 473.75 |
| DDD-66 | 474.0-480.0 | 475.25 | 478.83 | 479.75 |
| EEE-67 | 480.0-486.0 | 481.25 | 484.83 | 485.75 |
| FFF-68 | 486.0-492.0 | 487.25 | 490.83 | 491.75 |
| GGG-69 | 492.0-498.0 | 493.25 | 496.83 | 497.75 |
| HHH-70 | 498.0-504.0 | 499.25 | 502.83 | 503.75 |
| III-71 | 504.0-510.0 | 505.25 | 508.83 | 509.75 |
| JJJ-72 | 510.0-516.0 | 511.25 | 514.83 | 515.75 |
| KKK-73 | 516.0-522.0 | 517.25 | 520.83 | 521.75 |
| LLL-74 | 522.0-528.0 | 523.25 | 526.83 | 527.75 |
| MMM-75 | 528.0-534.0 | 529.25 | 532.83 | 533.75 |
| NNN-76 | 534.0-540.0 | 535.25 | 538.83 | 539.75 |
| OOO-77 | 540.0-546.0 | 541.25 | 544.83 | 545.75 |
| PPP-78 | 546.0-552.0 | 547.25 | 550.83 | 551.75 |
| QQQ-79 | 552.0-558.0 | 553.25 | 556.83 | 557.75 |
| RRR-80 | 558.0-564.0 | 559.25 | 562.83 | 563.75 |
| SSS-81 | 564.0-570.0 | 565.25 | 568.83 | 569.75 |

*Table D-1 NTSC Cable Television Channels and Relative Frequencies in MHz (continued)*

| Channel Number | Bandwidth | Video Carrier | Color Carrier | Audio Carrier |
|---|---|---|---|---|
| TTT-82 | 570.0-576.0 | 571.25 | 574.83 | 575.75 |
| UUU-83 | 576.0-582.0 | 577.25 | 580.83 | 581.75 |
| VVV-84 | 582.0-588.0 | 583.25 | 586.83 | 587.75 |
| WWW-85 | 588.0-594.0 | 589.25 | 592.83 | 593.75 |
| XXX86 | 594.0-600.0 | 595.25 | 598.83 | 599.75 |
| YYY-87 | 600.0-606.0 | 601.25 | 604.83 | 605.75 |
| ZZZ-88 | 606.0-612.0 | 607.25 | 610.83 | 611.75 |
| 89-89 | 612.0-618.0 | 613.25 | 616.83 | 617.75 |
| 90-90 | 618.0-624.0 | 619.25 | 622.83 | 623.75 |
| 91-91 | 624.0-630.0 | 625.25 | 628.83 | 629.75 |
| 92-92 | 630.0-636.0 | 631.25 | 634.83 | 635.75 |
| 93-93 | 636.0-642.0 | 637.25 | 640.83 | 641.75 |
| 94-94 | 642.0-648.0 | 643.25 | 646.83 | 647.75 |
| 100-100 | 648.0-654.0 | 649.25 | 652.83 | 653.75 |
| 101-101 | 654.0-660.0 | 655.25 | 658.83 | 659.75 |
| 102-102 | 660.0-666.0 | 661.25 | 664.83 | 665.75 |
| 103-103 | 666.0-672.0 | 667.25 | 670.83 | 671.75 |
| 104-104 | 672.0-678.0 | 673.25 | 676.83 | 677.75 |
| 105-105 | 678.0-684.0 | 679.25 | 682.83 | 683.75 |
| 106-106 | 684.0-690.0 | 685.25 | 688.83 | 689.75 |
| 107-107 | 690.0-696.0 | 691.25 | 694.83 | 695.75 |
| 108-108 | 696.0-702.0 | 697.25 | 700.83 | 701.75 |
| 109-109 | 702.0-708.0 | 703.25 | 706.83 | 707.75 |
| 110-110 | 708.0-714.0 | 709.25 | 712.83 | 713.75 |
| 111-111 | 714.0-720.0 | 715.25 | 718.83 | 719.75 |
| 112-112 | 720.0-726.0 | 721.25 | 724.83 | 725.75 |
| 113-113 | 726.0-732.0 | 727.25 | 730.83 | 731.75 |
| 114-114 | 732.0-738.0 | 733.25 | 736.83 | 737.75 |
| 115-115 | 738.0-744.0 | 739.25 | 742.83 | 743.75 |
| 116-116 | 744.0-750.0 | 745.25 | 748.83 | 749.75 |
| 117-117 | 750.0-756.0 | 751.25 | 754.83 | 755.75 |
| 118-118 | 756.0-762.0 | 757.25 | 760.83 | 761.75 |
| 119-119 | 762.0-768.0 | 763.25 | 766.83 | 767.75 |
| 120-120 | 768.0-674.0 | 769.25 | 772.83 | 773.75 |
| 121-121 | 774.0-780.0 | 775.25 | 778.83 | 779.75 |
| 122-122 | 780.0-786.0 | 781.25 | 784.83 | 785.75 |

*Table D-1 NTSC Cable Television Channels and Relative Frequencies in MHz (continued)*

| Channel Number | Bandwidth | Video Carrier | Color Carrier | Audio Carrier |
|---|---|---|---|---|
| 123-123 | 786.0-792.0 | 787.25 | 790.83 | 791.75 |
| 124-124 | 792.0-798.0 | 793.25 | 796.83 | 797.75 |
| 125-125 | 798.0-804.0 | 799.25 | 802.83 | 803.75 |
| 126-126 | 804.0-810.0 | 805.25 | 808.83 | 809.75 |
| 127-127 | 810.0-816.0 | 811.25 | 814.83 | 815.75 |
| 128-128 | 816.0-822.0 | 817.25 | 820.83 | 821.75 |
| 129-129 | 822.0-828.0 | 823.25 | 826.83 | 827.75 |
| 130-130 | 828.0-834.0 | 829.25 | 832.83 | 833.75 |
| 131-131 | 834.0-840.0 | 835.25 | 838.83 | 839.75 |
| 132-132 | 840.0-846.0 | 841.25 | 844.83 | 845.75 |
| 133-133 | 846.0-852.0 | 847.25 | 850.83 | 851.75 |
| 134-134 | 852.0-858.0 | 853.25 | 856.83 | 857.75 |
| 135-135 | 858.0-864.0 | 859.25 | 862.83 | 863.75 |
| 136-136 | 864.0-870.0 | 865.25 | 868.83 | 869.75 |
| 137-137 | 870.0-876.0 | 871.25 | 874.83 | 875.75 |
| 138-138 | 876.0-882.0 | 877.25 | 880.83 | 881.75 |
| 139-139 | 882.0-888.0 | 883.25 | 886.83 | 887.75 |
| 140-140 | 888.0-894.0 | 889.25 | 892.83 | 893.75 |
| 141-141 | 894.0-900.0 | 895.25 | 898.83 | 899.75 |
| 142-142 | 900.0-906.0 | 901.25 | 904.83 | 905.75 |
| 143-143 | 906.0-912.0 | 907.25 | 910.83 | 911.75 |
| 144-144 | 912.0-918.0 | 913.25 | 916.83 | 917.75 |
| 145-145 | 918.0-924.0 | 919.25 | 922.83 | 923.75 |
| 146-146 | 924.0-930.0 | 925.25 | 928.83 | 929.75 |
| 147-147 | 930.0-936.0 | 931.25 | 934.83 | 935.75 |
| 148-148 | 936.0-942.0 | 937.25 | 940.83 | 941.75 |
| 149-149 | 942.0-948.0 | 943.25 | 946.83 | 947.75 |
| 150-150 | 948.0-954.0 | 949.25 | 952.83 | 953.75 |
| 151-151 | 954.0-960.0 | 955.25 | 958.83 | 959.75 |
| 152-152 | 960.0-966.0 | 961.25 | 964.83 | 965.75 |
| 153-153 | 966.0-972.0 | 967.25 | 970.83 | 971.75 |
| 154-154 | 972.0-978.0 | 973.25 | 976.83 | 977.75 |
| 155-155 | 978.0-984.0 | 979.25 | 982.83 | 983.75 |
| 156-156 | 984.0-990.0 | 985.25 | 988.83 | 989.75 |
| 157-157 | 990.0-996.0 | 991.25 | 994.83 | 995.75 |
| 158-158 | 996.0-1002.0 | 997.25 | 1000.83 | 1001.75 |

*Table D-2 European Cable Television Channels and Relative Frequencies in MHz*

| Channel Number | Bandwidth | Video Carrier | Audio Carrier |
|---|---|---|---|
| 2 | 47-54 | 48.25 | 48.25 |
| 3 | 54-61 | 55.25 | 55.25 |
| 4 | 61-68 | 62.25 | 62.25 |
| S2 | 111-118 | 112.25 | 112.25 |
| S3 | 118-125 | 119.25 | 119.25 |
| S4 | 125-132 | 126.25 | 126.25 |
| S5 | 132-139 | 133.25 | 133.25 |
| S6 | 139-146 | 140.25 | 140.25 |
| S7 | 146-153 | 147.25 | 147.25 |
| S8 | 153-160 | 154.25 | 154.25 |
| S9 | 160-167 | 161.25 | 161.25 |
| S10 | 167-174 | 168.25 | 168.25 |
| 5 | 174-181 | 175.25 | 175.25 |
| 6 | 181-188 | 182.25 | 182.25 |
| 7 | 188-195 | 189.25 | 189.25 |
| 8 | 195-202 | 196.25 | 196.25 |
| 9 | 202-209 | 203.25 | 203.25 |
| 10 | 209-216 | 210.25 | 210.25 |
| 11 | 216-223 | 217.25 | 217.25 |
| 12 | 223-230 | 224.25 | 224.25 |
| S11 | 230-237 | 231.25 | 231.25 |
| S12 | 237-244 | 238.25 | 238.25 |
| S13 | 244-251 | 245.25 | 245.25 |
| S14 | 251-258 | 252.25 | 252.25 |
| S15 | 258-265 | 259.25 | 259.25 |
| S16 | 265-272 | 266.25 | 266.25 |
| S17 | 272-279 | 273.25 | 273.25 |
| S18 | 279-286 | 280.25 | 280.25 |
| S19 | 286-293 | 287.25 | 287.25 |
| S20 | 293-300 | 294.25 | 294.25 |
| S21 | 302-310 | 303.25 | 303.25 |
| S22 | 310-318 | 311.25 | 311.25 |
| S23 | 318-326 | 319.25 | 319.25 |
| S24 | 326-334 | 327.25 | 327.25 |
| S25 | 334-342 | 335.25 | 335.25 |
| S26 | 342-350 | 343.25 | 343.25 |

*Table D-2 European Cable Television Channels and Relative Frequencies in MHz (continued)*

| Channel Number | Bandwidth | Video Carrier | Audio Carrier |
|---|---|---|---|
| S27 | 350-358 | 351.25 | 351.25 |
| S28 | 358-366 | 359.25 | 359.25 |
| S29 | 366-374 | 367.25 | 367.25 |
| S30 | 374-382 | 375.25 | 375.25 |
| S31 | 382-390 | 383.25 | 383.25 |
| S32 | 390-398 | 391.25 | 391.25 |
| S33 | 398-406 | 399.25 | 399.25 |
| S34 | 406-414 | 407.25 | 407.25 |
| S35 | 414-422 | 415.25 | 415.25 |
| S36 | 422-430 | 423.25 | 423.25 |
| S37 | 430-438 | 431.25 | 431.25 |
| S38 | 438-446 | 439.25 | 439.25 |
| 21 | 470-478 | 471.25 | 471.25 |
| 22 | 478-486 | 479.25 | 479.25 |
| 23 | 486-494 | 487.25 | 487.25 |
| 24 | 494-502 | 495.25 | 495.25 |
| 25 | 502-510 | 503.25 | 503.25 |
| 26 | 510-518 | 511.25 | 511.25 |
| 27 | 518-526 | 519.25 | 519.25 |
| 28 | 526-534 | 527.25 | 527.25 |
| 29 | 534-542 | 535.25 | 535.25 |
| 30 | 542-550 | 543.25 | 543.25 |
| 31 | 550-558 | 551.25 | 551.25 |
| 32 | 558-566 | 559.25 | 559.25 |
| 33 | 566-574 | 567.25 | 567.25 |
| 34 | 574-582 | 575.25 | 575.25 |
| 35 | 582-590 | 583.25 | 583.25 |
| 36 | 590-598 | 591.25 | 591.25 |
| 37 | 598-606 | 599.25 | 599.25 |
| 38 | 606-614 | 607.25 | 607.25 |
| 39 | 614-622 | 615.25 | 615.25 |
| 40 | 622-630 | 623.25 | 623.25 |
| 41 | 630-638 | 631.25 | 631.25 |
| 42 | 638-646 | 639.25 | 639.25 |
| 43 | 646-654 | 647.25 | 647.25 |
| 44 | 654-662 | 655.25 | 655.25 |

*Table D-2 European Cable Television Channels and Relative Frequencies in MHz (continued)*

| Channel Number | Bandwidth | Video Carrier | Audio Carrier |
|---|---|---|---|
| 45 | 662-670 | 663.25 | 663.25 |
| 46 | 670-678 | 671.25 | 671.25 |
| 47 | 678-686 | 679.25 | 679.25 |
| 48 | 686-694 | 687.25 | 687.25 |
| 49 | 694-702 | 695.25 | 695.25 |
| 50 | 702-710 | 703.25 | 703.25 |
| 51 | 710-718 | 711.25 | 711.25 |
| 52 | 718-726 | 719.25 | 719.25 |
| 53 | 726-734 | 727.25 | 727.25 |
| 54 | 734-742 | 735.25 | 735.25 |
| 55 | 742-750 | 743.25 | 743.25 |
| 56 | 750-758 | 751.25 | 751.25 |
| 57 | 758-766 | 759.25 | 759.25 |
| 58 | 766-774 | 767.25 | 767.25 |
| 59 | 774-782 | 775.25 | 775.25 |
| 60 | 782-790 | 783.25 | 783.25 |
| 61 | 790-798 | 791.25 | 791.25 |
| 62 | 798-806 | 799.25 | 799.25 |
| 63 | 806-814 | 807.25 | 807.25 |
| 64 | 814-822 | 815.25 | 815.25 |
| 65 | 822-830 | 823.25 | 823.25 |
| 66 | 830-838 | 831.25 | 831.25 |
| 67 | 838-846 | 839.25 | 839.25 |
| 68 | 846-854 | 847.25 | 847.25 |
| 69 | 854-862 | 855.25 | 855.25 |

# Configuration Register Information for the Cisco uBR7200 Series Universal Broadband Routers

The following information is found in this appendix:


- Configuration Bit Meanings, page E-1
- Displaying the Configuration Register While Running Cisco IOS, page E-5
- Displaying the Configuration Register While Running ROM Monitor, page E-6
- Setting the Configuration Register While Running Cisco IOS, page E-6
- Setting the Configuration Register While Running ROM Monitor, page E-7


## Configuration Bit Meanings

Use the processor configuration register information contained in this appendix to do the following:

- Set and display the configuration register value
- Force the system into the bootstrap program
- Select a boot source and default boot filename
- Enable or disable the Break function
- Control broadcast addresses
- Set the console terminal baud rate
- Load operating software from ROM
- Enable booting from a Trivial File Transfer Protocol (TFTP) server

Table E-1 lists the meaning of each of the configuration memory bits. Following the table is a more in-depth description of each setting.

*Table E-1 Configuration Register Bit Settings*

| Bit No. | Hex | Meaning |
|---|---|---|
| 00–03 | 0x0000–0x000F | Boot field |
| 06 | 0x0040 | Causes the system software to ignore nonvolatile random-access memory (NVRAM) contents |
| 07 | 0x0080 | OEM (original equipment manufacturer) bit enabled |

*Table E-1 Configuration Register Bit Settings (continued)*

| Bit No. | Hex | Meaning |
|---|---|---|
| 08 | 0x0100 | Break disabled |
| 10 | 0x0400 | IP broadcast with all zeros |
| 11–12 | 0x800–0x1000 | Console line speed |
| 13 | 0x2000 | Boots default ROM software if initial boot fails |
| 14 | 0x4000 | IP broadcasts do not have network numbers |
| 15 | 0x8000 | Enables diagnostic messages and ignores NVRAM contents |

# Bits 0–3

The lowest four bits of the processor configuration register (bits 3, 2, 1, and 0) form the boot field. Table E-2 provides information about the bits settings.

*Table E-2 Bits 0–3 Settings*

| Boot Field | Meaning |
|---|---|
| 0 | Stays at the system bootstrap prompt (ROM monitor) on a reload or power cycle |
| 1 | Boots the boot helper image as a system image |
| 2 | Full boot process, which loads the Cisco IOS image into Flash memory |
| 2-F | Specifies a default filename for booting over the network from a TFTP server |

The boot field specifies a number in binary. If you set the boot field value to 0, you must have a console port access to boot the operating system manually. Boot the operating system by entering the **b** command at the bootstrap prompt as follows:

```
> b [tftp] flash filename
```

Definitions of the various command options follow:

**b**—Boots the default system software from ROM

**b flash**—Boots the first file in Flash memory

**b** *filename [host]*—Boots over the network using TFTP

**b flash** *filename*—Boots the file (*filename*) from Flash memory

If you set the boot field value to a value of 2 through F, and there is a valid system boot command stored in the configuration file, the router boots the system software as directed by that value. (See Table E-3.) If you set the boot field to any other bit pattern, the router uses the resulting number to form a default boot filename for netbooting.

If there are no **boot** commands in the configuration file, the router attempts to boot the first file in system Flash memory. If no file is found in system Flash memory, the router attempts to netboot a default file with a name derived from the value of the boot field (for example, cisco2-7200). If the netboot attempt fails, the boot helper image in boot flash memory will boot up.

If **boot** commands are in the configuration file, the router software processes each **boot** command in sequence until the process is successful or the end of the list is reached. If the end of the list is reached without a file being successfully booted, the router will retry the **netboot** commands up to six times if bit 13 of the configuration register is set, otherwise it will load the operating system software available

in ROMmon. If bit 13 is not set, the router will continue to netboot images indefinitely. The default setting for bit 13 is 0. If bit 13 is set, the system boots the boot helper image found in boot flash memory without any retries.

The server creates a default filename as part of the automatic configuration processes. To form the boot filename, the server starts with Cisco and links the octal equivalent of the boot field number, a dash, and the image name. Table E-3 lists the default boot filenames or actions.

Note A **boot system configuration** command in the router configuration in NVRAM overrides the default netboot filename.

*Table E-3 Default Boot Filenames*

| Action/File Name | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
|---|---|---|---|---|
| Bootstrap mode | 0 | 0 | 0 | 0 |
| ROM software | 0 | 0 | 0 | 1 |
| Flash software | 0 | 0 | 1 | 0 |
| cisco3-< image-name1> | 0 | 0 | 1 | 1 |
| cisco4-<image-name2> | 0 | 1 | 0 | 0 |
| cisco5-<image-name3> | 0 | 1 | 0 | 1 |
| cisco6-<image-name4> | 0 | 1 | 1 | 0 |
| cisco7-<image-name5> | 0 | 1 | 1 | 1 |
| cisco10-<image-name6> | 1 | 0 | 0 | 0 |
| cisco11-<image-name7> | 1 | 0 | 0 | 1 |
| cisco12-<image-name8> | 1 | 0 | 1 | 0 |
| cisco13-<image-name9> | 1 | 0 | 1 | 1 |
| cisco14-<image-name10> | 1 | 1 | 0 | 0 |
| cisco15-<image-name11> | 1 | 1 | 0 | 1 |
| cisco16-<image-name12> | 1 | 1 | 1 | 0 |
| cisco17-<image-name13> | 1 | 1 | 1 | 1 |

## Bit 6

Bit 6 causes the system software to ignore nonvolatile random-access memory (NVRAM) contents.

## Bit 7

Bit 7 enables the OEM bit. It disables the bootstrap messages at startup.

## Bit 8

Bit 8 controls the console Break key. Setting bit 8 (the factory default) causes the processor to ignore the console Break key. Clearing bit 8 causes the processor to interpret Break as a command to force the system into the bootstrap monitor, halting normal operation. A Break can be sent in the first sixty seconds while the system reboots, regardless of the configuration settings.

# Bit 10 and Bit 14

Bit 10 controls the host portion of the Internet IP broadcast address. Setting bit 10 causes the processor to use all zeros; clearing bit 10 (the factory default) causes the processor to use all ones. B it 10 interacts with bit 14, which controls the network and subnet portions of the IP broadcast address. Table E-4 shows the combined effect of bit 10 and bit 14.

*Table E-4 Bit 10 and Bit 14 Settings*

| Bit 14 | Bit 10 | IP Address (<net> <host>) |
|---|---|---|
| Off | Off | <ones><ones> |
| Off | On | <zeros><zeros> |
| On | On | <net><zeros> |
| On | Off | <net><ones> |

Note The console line rate on Cisco universal broadband routers is fixed at 9600 and cannot be changed. For additional information about configuring baud rates, refer to oneor more of these documents on Cisco.com:

- "Using the ROM Monitor on the Cisco CMTS" in the *Cisco Broadband Cable Command Reference Guide*:

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_command_reference_chapter09186a0080187230.html

# Bit 11 and Bit 12

Bit 11 and Bit 12 in the configuration register determine the baud rate of the console terminal. Table E-5 shows the bit settings for the four available baud rates. (The factory set default baud rate is 9600.)

*Table E-5 Bit 11 and Bit 12 Settings*

| Baud | Bit 12 | Bit 11 |
|---|---|---|
| 9600 | 0 | 0 |
| 4800 | 0 | 1 |
| 2400 | 1 | 1 |
| 1200 | 1 | 0 |

Note The console line rate on Cisco universal broadband routers is fixed at 9600 and cannot be changed. For additional information about configuring baud rates, refer to oneor more of these documents on Cisco.com:

- "Using the ROM Monitor on the Cisco CMTS" in the *Cisco Broadband Cable Command Reference Guide*:

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_command_reference_chapter09186a0080187230.html

## Bit 13

Bit 13 determines the server response to a bootload failure. If **boot** commands are in the configuration file, the router software processes each **boot** command in sequence until the process is successful or the end of the list is reached. If the end of the list is reached without a file being successfully booted, the router will retry the **netboot** commands up to six times if bit 13 of the configuration register is set, otherwise it will load the operating system software available in ROMmon. If bit 13 is not set, the router will continue to netboot images indefinitely. The default setting for bit 13 is 0. If bit 13 is set, the system boots the boot helper image found in boot flash memory without any retries.

## Bit 15

Bit 15 enables diagnostic messages and ignores NVRAM contents.

# Displaying the Configuration Register While Running Cisco IOS

The configuration register can be viewed by using the **show version** or **show hardware** command.

The following example illustrates output from the **show version** command for a Cisco uBR7246 VXR router with the cable clock card installed:

```
Router# show version

Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (UBR7200-P-M), Version 12.1(10)EC, RELEASE SOFTWARE
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Wed 02-Feb-00 16:49 by ccai
Image text-base:0x60008900, data-base:0x61192000

ROM:System Bootstrap, Version 12.0(15)SC, RELEASE SOFTWARE

VXR1 uptime is 2 days, 1 hour, 24 minutes
System returned to ROM by power-on at 10:54:38 PST Sat Feb 5 2000
System restarted at 11:01:08 PST Sat Feb 5 2000
System image file is "slot1:ubr7200-p-mz.121-0.8.T"

cisco uBR7246VXR (NPE300) processor (revision B) with 122880K/40960K bytes of memory.
Processor board ID SAB0329005N
R7000 CPU at 262Mhz, Implementation 39, Rev 1.0, 256KB L2, 2048KB L3 Cache
6 slot VXR midplane, Version 2.0

Last reset from power-on
X.25 software, Version 3.0.0.
National clock card with T1 controller
1 FastEthernet/IEEE 802.3 interface(s)
2 Cable Modem network interface(s)
125K bytes of non-volatile configuration memory.

16384K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
20480K bytes of Flash PCMCIA card at slot 1 (Sector size 128K).
4096K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x0

Router#
```

# Displaying the Configuration Register While Running ROM Monitor

If the bootstrap prompt ">", the **o** command displays the virtual configuration register currently in effect. It includes a description of the bits. See the following sample output:

```
>o
Configuration register + 02x100 at last boot
Bit#       Configuration register option settings:
15         Diagnostic mode disabled
14         IP broadcasts do not have network numbers
13         Boot default ROM software if network boot fails
12-11      Console speed is 9600 baud
10         IP broadcasts with ones
09         Do not use secondary bootstrap
08         Break disabled
07         OEM disabled
06         Ignore configuration disabled
05         Fast boot disabled
04         Fan boot disabled
03-00      Boot to ROM monitor
```

If the prompt is "rommon1", the **confreg** command displays the virtual configuration register currently in effect. It includes a description of the bits. See the following sample output:

```
rommon 1 > confreg

Configuration Summary
enabled are:
load rom after netboot fails
console baud: 9600
boot: the ROM Monitor

Do you wish to change the configuration? y/n  [n]
```

# Setting the Configuration Register While Running Cisco IOS

The configuration register can be set in the configuration mode with the **config-register 0x**<value> command. See the following sample output:

```
Router# config t
Enter configuration commands, one per line. End with CNTRL/Z.
Router(config)#config-register 0x2142
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

# Setting the Configuration Register While Running ROM Monitor

If the prompt is ">", the **or0x**<value> command sets the configuration register. See the following sample output:

```
>o/r 0x2102
>
```

If the prompt is "rommon1", the **confreg** command sets the configuration register. It prompts the user about each bit. See the following sample output:

```
rommon 1 > confreg

Confiuration Summary
enabled are:
load rom after netboot fails
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration y/n    [n]:  y
enable  "diagnostic mode"? y/n   [n]:   n
enable   "use net in IP bcast address"? y/n  [n]:   n
disable  "use rom after netboot fails"? y/n  [n]:  n
enable   "use all zero broadcast"? y/n  [n]:  n
enable   "break/abort has effect"? y/n  [n]:  n
enable   "ignore system config info"? y/n   [n]:  n
change console baud rate? y/n  [n]:  n
change the boot characteristics? y/n   [n]:y
enter to boot:
0 = ROM Monitor
1 = the boot helper image
2 - 15 = boot system
    [0]: 2

Configuration Summary:
enabled are:
load rom after netboot fails
console baud: 9600
boot: image sepcified by the boot system commands or default to: cisco2-c7200

do you wish to change the configuration? y/n   [n]   n

You must reset or power cycle for new config to take effect
rommon 2 >
```

## A


access control lists (ACL) 1-108
  COPS Intercept support 1-73
acronyms, list of xiv
address
  CM upstream address verification 5-4
  downstream helper address 3-7
  dynamic IP address allocation 1-32
addresses, MAC 1-17
address verification
  upstream 1-64
admission control 1-86, 3-12, 3-13
algorithm
  amplitude averaging 8-7
  automatic dynamic backoff 3-19
  downstream rate limiting 3-10
  dynamic backoff 5-7
  dynamic contention algorithm 5-6
  dynamic map advance 5-7
  upstream rate limiting 3-26
amplitude averaging 8-7
ARP (Address Resolution Protocol)
  debug cable arp command 8-11
  downstream requests 3-2, 3-3
  host-to-host communication, activating Proxy ARP 3-28
AutoInstall
  facility overview 1-31
Autoinstall facility
  configuring Cisco uBR7200 series with 2-10


## B


backoff values, upstream 3-19, 3-20
bandwidth management 1-33
Baseline Privacy Interface (BPI)
  BPI network example 4-2
  CM communication with 4-3
  configuration files 2-29
  debug cable keyman command 8-12
  debug cable privacy command 8-13
  differentiating traffic streams 4-3
  enabling 4-3
  encrypted data on the cable TV network 4-3
  encryption and encrypted key exchange 1-49
  key management 4-2
  overview 4-1
Baseline Privacy Interface Plus (BPI+)
  overview 4-4
boot
  reboot router 2-9
broadband Internet access
  configuring 6-1
  overview 6-1
  recommended configuration 6-2
  sample configuration file 6-3
broadcast echo 3-34


## C


cable commands
  cable bundle master 3-31
  cable device 1-129
  cable dhcp-giaddr 1-59

cable downstream annex 3-9
cable downstream channel-id 3-5
cable downstream frequency 3-5
cable downstream if-output 3-4, 8-9
cable downstream interleave-depth 3-8
cable downstream modulation 3-9
cable downstream override 1-123
cable downstream rate-limit token-bucket 3-6, 3-10
cable helper-address 3-7
cable host 1-129
cable insertion-interval 1-141
cable intercept 1-81
cable map-advance 1-89
cable modem remote-query 1-111
cable modulation-profile 1-58, 2-22
cable monitor 1-90
cable registration-timeout 5-6
cable source-verify 1-103
cable-source verify dhcp 1-47
cable spectrum-group 2-22
cable sync-interval 5-9
cable upstream 3-16
cable upstream admission-control 3-13
cable upstream channel-width 3-21
cable upstream data-backoff 1-141, 3-19
cable upstream differential-encoding 3-13
cable upstream fec 3-14
cable upstream freq-adj averaging 8-8
cable upstream frequency 1-16, 3-22
cable upstream frequency-adjust averaging 3-15
cable upstream minislot-size 3-25
cable upstream modulation-profile 1-121
cable upstream power-adjust 3-16, 8-7
cable upstream power-level 3-24
cable upstream range backoff 1-141
cable upstream rate-limit 3-18
cable upstream rate-limit token-bucket 3-26
cable upstream scrambler 3-17
cable upstream time-adjust 3-17
cable interface
  configuring 3-1
  downstream, configuring 3-2
  Setup facility 1-31
  upstream, configuring 3-11, 3-22
cable interface line card
  logical interface numbering 1-15
  slot numbering 1-15
cable modem
  authentication
    activating 5-2
    troubleshooting 5-3
    verifying 5-2
  configuring cable modem interface 3-1
  configuring registration timeout 5-6
  counters, clearing 5-5
  dynamic contention algorithms 5-6
  hosts, configuring maximum configurable hosts 5-8
  insertion interval 5-3, 5-6
  registration timeout, configuring 5-6
  reset, clearing 5-5
  sync message interval, configuring 5-9
  troubleshooting 1-123
  troubleshooting, verifying downstream signals 8-6
  upstream address verification, activating 5-4
Cable Modem Termination System
  see CMTS
Cable Modulation Profile Default Templates 1-58
Cable Monitor Enhancements 1-73
channel ID, downstream
  configuring 3-5
  verifying 3-6
channel width, upstream
  configuring 3-21
Cisco IOS
  features 1-22
Cisco Network Registrar, see CNR
clear commands
  clear cable host 1-129

clear cable modem counters 5-5
clear cable modem reset 1-91, 5-5
CMTS (Cable Modem Termination System)
configuring global parameters 2-18
configuring manually with Configuration mode 2-27
configuring with AutoInstall facility 2-10
configuring with Extended Setup facility 2-25
configuring with Setup facility 2-17
preconfiguring 2-2
CNR (Cisco Network Registrar)
activating scripts 7-4
class of service (CoS) policies 7-7
default policy 7-5
network scopes 7-6
overview 7-1
script overview 7-3
tag scopes 7-5
Configurable Leasequery Server 1-47
configuration bit meanings E-1
configuration facilities and modes 1-31
configuration files
reviewing modifications 2-29
samples 2-29, C-1
saving 2-13, 2-29
Configuration mode
configuring CMTS with 2-27
configuration register E-1
configure commands
configure memory 2-9
configure terminal 2-9, 2-22, 2-28, 3-3, A-4
COPS Intercept
Access Control List support 1-73
TCP support 1-74
copy commands
copy rcp flash A-2, A-4
copy running-config startup-config 2-9, 2-11, 2-13, 2-29
copy running-config tftp 2-15
copy running start 1-16
copy slot A-4
copy tftp flash A-2, A-4
counters
clearing cable modem 5-5


## D


Data Encryption Standard (DES)
changing default 2-30
debug commands
debug cable arp command 8-11
debug cable error command 3-33
debug cable keyman 8-12
debug cable phs command 3-33
debug cable privacy 8-13
DHCP (Dynamic Host Configuration Protocol)
address pools 6-3
cable modem leases 5-4
DHCP client ID/remote ID options 1-59
DHCP server 1-59
MAC address exclusion list 1-47
server in preconfiguration 2-3
DHCP cable modem host ID 1-59
differential encoding 3-13, 3-14
DOCSIS
Annex B 3-9
DOCSIS CPE Configurator, V2.0.4 1-53
DOCSIS CPE Configurator, V3.2 1-53
MPEG framing format 3-9
ping docsis command 8-10
DOCSIS 1.0
Baseline Privacy Interface (BPI) 1-49, 4-1
Quality of Service prior to DOCSIS 1.1 1-52
supported features on Cisco uBR7200 series 1-49
DOCSIS 1.0+
supported features on Cisco uBR7200 series 1-56
DOCSIS 1.1
Baseline Privacy Interface Plus (BPI+) 4-4
certification for uBR7246VXR on Cisco IOS release 12.2(4)BC1 1-4

Quality of Service 1-60
service flow model 1-60
Set-Top Gateway Issue 1-87
supported features on Cisco uBR7200 series 1-57
token-bucket rate shaping 3-10, 3-26
two-way transmission 1-65
DOCSIS 2.0
supported features on Cisco uBR7200 series 1-67
DOCSIS 2.0 SAMIS ECR Data Set 1-90
downstream
cable ARP requests, activating 3-2
channel ID
configuring 3-5
verifying 3-6
CM interface, configuring 3-2
downstream frequency override 1-65
downstream modulation 3-8
downstream rate shaping with IP type of service bits 1-66
helper address 3-7
interleave depth 3-8
MPEG framing format 3-9, 3-10
ports 3-3, 3-4
rate limiting 3-10
troubleshooting downstream CM signals 8-6
DRP (Director Response Protocol), server agent 1-68
DSG 1.1 1-87
DSX Messages and Synchronized PHS Information 1-69
dynamic backoff algorithm 5-7
Dynamic Channel Change (DCC) for Loadbalancing 1-90
dynamic contention algorithms 5-6
dynamic map advance algorithm 5-7
dynamic ranging 3-19
Dynamic SID/VRF Mapping Support 1-127


## E


Easy IP (phase 1) 1-83
echo, IP broadcast and IP multicast 1-79
EEPROM, MAC address bank 1-17
examples
Internet access C-1, C-3
IP telephony (VoIP) C-12
sample configuration files C-1
show interfaces command output 1-19, 1-21
telco return C-14
virtual private network (VPN) C-9
exec prompt timestamp command 1-33
Extended Setup facility
configuring Cisco uBR7200 series with 2-25


## F


figures
Two-way Internet access network example 6-2
framing format, MPEG 3-9, 3-10
frequency, setting upstream 3-22, 3-23


## G


Globally Configured HCCP 4+1 Redundancy 1-69
global parameters, configuring 2-18
GRE tunnels 1-127


## H


hardware address 1-17
helper address, downstream 3-7
High Availability Features 1-68
High Availability Support for Encrypted IP Multicast 1-71
host-to-host communication (Proxy ARP) 3-28
HSRP (Hot Standby Router Protocol) 1-126


## I


IGRP (Interior Gateway Routing Protocol)
authentication 1-84

IGRP (Internet Gateway Routing Protocol)
IP Enhanced IGRP Route Authentication 1-84
IP routing with 2-20
input power level, upstream 3-24
insertion interval, cable modem 5-6
Intercept
COPS Intercept 1-73
COPS TCP Support 1-74
Service Independent Intercept 1-78
Interior Gateway Routing Protocol
See IGRP
interleave depth, downstream 3-8
IP
broadcast echo 1-79, 3-34
Easy IP (phase 1) 1-83
IP broadcast echo 3-34
IP enhanced IGRP route authentication 1-84
IP multicast echo 3-33
IP parameters, setting optional 3-33
IP routing features supported on Cisco uBR7200 series 1-80
IP type-of-service and precedence for GRE tunnels 1-127
multicast echo 3-34
Network Address Translation (NAT) 1-84
setting routing protocols for 2-20
IPv6 over L2VPN 1-127

## K

key encryption key (KEK) 2-30

## M

MAC (Media Access Control)
configuring PHS 3-33
Management Information Base (MIB) Changes and Enhancements 1-93
minislot 3-25
modem
see cable modem
modulation, downstream 3-8
MPEG, downstream framing format 3-9, 3-10
multicast echo 3-33, 3-34
multicast options 1-98
Multilink Point-to-Point Protocol (MLPPP) 1-134

## N

NAT (Network Address Translation) 1-84
Network-Based Application Recognition (NBAR) 1-46
Network Time Protocol (NTP) 1-115
numbering
cable interface line card slot 1-15
logical interface 1-15
port adapter slot 1-15
NVRAM (Nonvolatile Random-Access Memory), saving and viewing contents in 2-29

## P

Packet Cable 1-101
packet interception 3-29
Parser Cache 1-34
parser cache command 1-34
password 2-6
passwords
password recovery process 2-7
setting password protection 2-5
PHS (Payload Header Suppression)
configuring 3-33
overview 1-62
ping docsis command 8-10
port adapters
logical interface numbering 1-15
slot numbering 1-15
ports, downstream 3-3, 3-4
ports, upstream 3-15

power adjustment 3-16, 3-17
power level 3-24
PPPoE (Point-to-Point Protocol over Ethernet) 1-135
Pre-equalization Control for Cable Modems 1-94
protocols
  ARP (Address Resolution Protocol)
    downstream, activating 3-2
    downstream, verifying 3-3
    Proxy ARP 3-28
  Bootstrap Protocol (BOOTP) 1-31
  Dynamic Host Configuration Protocol (DHCP) 1-31
  IGRP (Internet Gateway Routing Protocol) 2-20
  Internet Protocol (IP) 1-8
  Multicast Source Discovery Protocol (MSDP) 1-115
  Network Time Protocol (NTP) 1-115
  Real-Time Transport Protocol (RTP) 1-46
  RIP (Routing Information Protocol) 2-20
  Simple Network Management Protocol (SNMP) 1-110
  Trivial File Transfer Protocol (TFTP) 1-31, 1-63
Proxy ARP 3-28

## Q

Quality of Service
  Cisco 1-45
  DOCSIS 1.1 1-60
  DOCSIS enhancements prior to DOCSIS 1.1 1-52

## R

rate limiting
  downstream 3-10
  upstream 3-26, 3-27
reboot, router 2-9
registration timeout 5-6
RIP (Routing Information Protocol) 2-20
RTP Header Compression 1-46

## S

sample configuration files 2-29, C-1
scrambler, activating 3-17
security
  features 1-102
  replacing or recovering a lost password 2-6
  setting password protection 2-5
Service Independent Intercept 1-78
Setup facility 1-31
  configuring Cisco uBR7200 series with 2-17
show commands
  show cable bundle forwarding-table 3-31
  show cable device 1-129
  show cable host 1-129
  show cable modem 1-35, 5-5, 8-7
  show cable modem summary 1-35
  show cable modulation-profile 1-35
  show cable qos 1-35
  show cable tech-support 1-41
  show controllers cable 1-42
  show controllers cable downstream 3-6
  show int cx/y sid 1-35
  show interface cable 3-33
  show interfaces 1-19, 1-20
  show interfaces cable 1-19
  show running-config 1-16, 3-10, 3-17
  show slot A-4
  show tech support 1-44
  understanding show command responses 8-2
slot/port numbers for interfaces 1-17
SNMP features 1-109
spectrum management 1-119
status, cable interface 2-26
  downstream 1-19
  upstream 1-20
symbols, defined xiv
sync message interval 5-9

## T

terms and acronyms xiv
TFTP (Trivial File Transfer Protocol)
  overview 1-63
  TFTP server 2-3, A-1, B-1
Time-of-Day Server 1-62
timesaver symbol, defined xiv
timing adjustment, upstream 3-17, 3-18
ToD (time-of-day) server 2-3
token-bucket rate shaping 3-10, 3-26
traffic encryption key (TEK) 2-30
troubleshooting
  amplitude averaging 8-7
  cable flap list 1-123
  downstream frequency 1-123
  downstream signals 8-6
  fast fault detection 1-123
  static CPE 1-123
  upstream rate limiting 3-27
Turbo ACL (Access Control Lists) 1-108
Type/Length/Value Parser and Encoder 1-63

## U

upstream
  address verification 1-64
  admission control 3-12, 3-13
  backoff values 3-19, 3-20
  cable interface 3-11, 3-22
  channel width, configuring 3-21
  differential encoding 3-13, 3-14
  FEC (forward error correction) 3-14
  frequency 3-22, 3-23
  input power level 3-24
  minislot size 3-25
  ports 3-15
  power adjustment 3-16, 3-17
  rate limiting 3-26, 3-27
  scrambler 3-17
  scrambler, activating 3-17
  timing adjustment 3-17, 3-18
upstream frequency adjustment
  configuring 3-15

## V

virtual interface
  bundling 1-125
voice support 1-101